Joint Planning and Development Office

Integrated Air Surveillance Concept of Operations

November 2011

Next Generation Air Transportation System
Joint Planning and Development Office

Integrated Air Surveillance Concept of Operations

Revision Approval Record

Joint Planning and Development Office	**Karlin Toner**
Department of Defense	**Robert Salesses**
Department of Commerce/National Oceanic and Atmospheric Administration	**Samuel Williamson**
Department of Homeland Security	**Alan Cohn**
Federal Aviation Administration	**Michael Huerta**
Office of the Director for National Intelligence	**Guy Turner**

November 2011

Document Revision History

Version	Document Content Added	Reviewer	Release Date
2.1	Modifications to incorporate major community comments	Integrated Surveillance (IS) Community	23 April 2009
2.2	Modifications to incorporate major community comments	IS Community	04 May 2009
3.0	Modifications to incorporate major community comments	IS Community	16 June 2009
4.0	Internal Integrated Surveillance Analysis Team (ISAT) Review	Integrated Surveillance Analysis Team	18 May 2011
4.01	Revisions based on ISAT review	IS Community	26 May 2011
4.02	Revisions based on IS Community Review	IS Community	24 June 2011
4.03	Revisions based on IS Community Review	Senior Advisors	20 July 2011
4.04	Revisions based on IS Community Review	Senior Advisors	29 Aug 2011
4.05	Revisions based on IS Senior Advisors Review	Senior Advisors	30 Aug 2011

Acknowledgements

Many IS practitioners have given generously of their time and expertise to work with the Joint Planning and Development Office (JPDO) NextGen Integrated Surveillance Analysis Team (ISAT) in developing the Integrated Surveillance (IS) Concept of Operations (ConOps). Version 4 reflects requirements and desired capabilities of those partners who work in close collaboration across federal, state, and local organizations to keep the Nation's air space secure and safe. We thank them all for their shared insights and believe that such collaborative efforts now can spur real progress in the future. The following tables list these participants and their contributions:

Participants in the IS ConOps Revision Process

Agency	Participants
Department of Commerce (DOC)	Mr. Daniel Melendez, NOAA Mr. Bob Saffle, NOAA / Noblis Inc. Mr. Benjie Spencer, NOAA Mr. Jud Stailey, NOAA
Department of Defense (DoD)	Lt Col Tom Alto, NORAD-USNORTHCOM Lt Col Campbell, EADS Lt. Col Chas Cox, NORAD-USNORTHCOM Lt Col Filkorn, EADS Mr. Glenn Gese, NORAD-USNORTHCOM Mr. Willie Harris, JIAMDO Mr. Rick Hensley, NORAD-USNORTHCOM Lt. Col Pat Holleran, NORAD-USNORTHCOM Mr. Bill Mullins, USAF HQ Lt Col Rodder, EADS Mr. Steve Ruggles, NORAD-USNORTHCOM / Booz Allen Hamilton Mr. Harry Smythe, NORAD-USNORTHCOM Lt Col Merryl Tengesdal, NORAD-USNORTHCOM Lt Col Ann Wong, JIAMDO Mr. Brandon Wood, NORAD-USNORTHCOM
Federal Aviation Administration (FAA)	Mr. James Baird, NAS EA Group Ms. Michelle Merkle, ATS Concept &Validation Development Mr. Gary Miller, Tactical Operations Security Group Ms. Lisa Smith Ms. Jennifer Wahal

Department of Homeland Security (DHS)	Mr. Craig Benshoof, AMOC Mr. John Bioty, DHS HQ / Booz Allen Hamilton Mr. Bruce Browne, TSA/NCRCC Mr. Mitch Crosswait, DHS HQ Mr. Robin Dooley, AMOC Ms. Dianna Davis, TSA Col William Durham, CBP Mr. Jim Durrett, AMOC Mr. Chris Featherstone, DHS HQ Mr. Hal Frasch, CBP Ms. Cristal Frinell, AMOC Ms. Kim Garcia, AMOC, Intelligence Mr. Dan Hicken, FAA liaison, AMOC Mr. Bob Keller, AMOC, Intelligence Mr. Ron Kissinger, AMOC Ms. Diana Knittle, AMOC Mr. Chuck Larir SDEO, AMOC Ms. Virginia Lariviere, AMOC Mr. Jeff Mayer SDEO, AMOC Mr. Clinton Preston, DHS HQ Mr. Francisco Quesada, AMOC Mr. Julian Ross, DHS HQ Mr. Joe Anello, DHS HQ Mr. Randy Talley, DHS HQ Mr. Stephen Roulle AMOC Ms. Sherry Zeigler, AMOC
Office of the Director of National Intelligence (ODNI)	Mr. Josh Holtzman

JPDO NextGen Integrated Surveillance Analysis Team

Participants	Role
Patricia Craighill	JPDO Assistant Director – Defense, Special Advisor to the Chief, Warfighting Integration and CIO
Peggy Gervasi	Director, JPDO Strategic Interagency Initiatives Division
Diana Takata	JPDO Chief Architect (Acting)
Wanda Jones-Heath	Deputy Director, JPDO Net-Centric Operations Division
Stephen Irmo	JPDO IS ConOps Revision Federal Lead
Claude Speed	IS ConOps Revision Contractor Lead / Alion Science and Technology
Uriel Moore	IS ConOps Revision Support / Alion Science and Technology
Dale DeKinder	IS ConOps Revision Support / 5D Consulting LLC
Shawn Herron	IS ConOps Revision Support / Booz Allen Hamilton
Beth Huffer	IS ConOps Revision Support / Concept Solutions

Terry Moss	IS ConOps Revision Support / Alion Science and Technology
Emily Brandes	IS ConOps Revision Support / Concept Solutions
Jerry Friedman	IS ConOps Revision Support / MITRE
Avinash Pinto	IS ConOps Revision Support / MITRE

Table of Contents

Table of Figures

Preface

The United States Government conducts air surveillance operations to encourage and allow maximum appropriate use of United States airspace and to maintain the safety, security and defense of the homeland. Given the complexity of the National Airspace System (NAS), and the ever increasing volume of air traffic, meeting these objectives is a multi-agency responsibility. The Surveillance Mission Partners - the Departments of Transportation, Defense, Homeland Security and Commerce,[1] supported by the Office of the Director of National Intelligence - all have vital roles to play. Better integration of the surveillance mission partners' operations and systems is needed to ensure that they can continue to carry out their respective missions effectively. Integrated air surveillance is defined as the integration of information from cooperative and non-cooperative surveillance systems to create a user-defined operational picture, from common information, of real or near-real time situation for safety, security, and efficiency.[2]

In December 2008, participants at the Interagency Surveillance Summit[3], hosted by the Deputy Secretary of Homeland Security, requested development of an Integrated Air Surveillance Concept of Operations (IS ConOps) drawn from existing ConOps-related documents, an initial Integrated Surveillance Enterprise Architecture (ISEA) and a governance recommendation. The Next Generation Air Transportation System (NextGen) Joint Planning and Development Office (JPDO) was tasked to prepare those products.

In July 2010, the JPDO's oversight body, the Senior Policy Committee [4](SPC), directed that the recommended governance mechanism and work plan be put into action and that the IS ConOps be updated with the specific intent of resolving the outstanding issues that had prevented total concurrence in draft version 3.0.

This update to the IS ConOps identifies shared requirements for joint capabilities and changes needed to effect a transition from today's evolving collaborative environments to a fully and deliberately integrated, interagency air surveillance "system of systems". Key attributes of the NextGen strategy to improve air surveillance capabilities include:

- Leveraging existing surveillance assets to provide optimal, persistent, wide area surveillance coverage of key sectors of the United States airspace and approaches, with

[1] Integrated Surveillance for the Next Generation Air Transportation System: Final Report of the Integrated Surveillance Study Team, October 31, 2008.

[2] Final Report of the Integrated Surveillance Study Team, October 31, 2008.

[3] Summit attendees included senior leaders from the FAA, National Oceanic and Atmospheric Administration, JPDO, DHS, the United States Air Force, NORAD-NORTHCOM, National Guard Bureau, ODNI, Air Force North, and the National Security Staff.

[4] The Senior Policy Committee is chaired by the Secretary of Transportation and includes the Secretary of Homeland Security, the FAA Administrator, the Director of the White House Office of Science and Technology, the Secretary of Commerce, the NASA Administrator, the Secretary of the United States Air Force, and the Office of the Director of National Intelligence (ex-officio).

the longer-term goal of providing coverage of the entirety of United States airspace (refer to *Appendix A* and *Appendix D* for requirements specificity)
- Developing an interagency, information sharing infrastructure that enables seamless sharing of surveillance data and other relevant information through machine-to-machine interfaces, to ensure access to data by all authorized consumers and to maintain data integrity, provenance, and security
- Encouraging and facilitating development of automated data correlation, fusion, filtering and analysis tools, to alleviate information overload and to reduce the burden on operators of conducting time-consuming and labor-intensive manual information management tasks

In order to deliver this capability, key governance and policy issues must be addressed by the Air Domain Awareness Board (ADAB), including:

- Conduct acquisition, research and development, and maintenance activities that consider the requirements, capabilities and architectures of all surveillance mission partners, and equitably allocate responsibilities and costs for shared infrastructure and services
- Review, approve, and implement multi-layer security policies that impact interagency interoperability

The near-term strategy described in this IS ConOps is consistent with the long-term 2025 NextGen vision for NAS air traffic management, security, law enforcement, and defense needs. It complements the ADA initiative, which is creating an ADA Operational Concept (OpsCon) document.

1 Introduction

Effective operation of the NAS for civil aviation, national defense, homeland security, and other aviation security activities (e.g., law enforcement) relies on accurate and timely airspace situational awareness supported by surveillance capabilities. Integrated air surveillance is defined as the combination of information from cooperative and non-cooperative surveillance systems to create a user-defined operational picture (from common information) of real or near-real time situation for safety, security, and efficiency.[5] To this end, individual agencies within the United States Government have made varying progress toward fielding advanced surveillance and situational awareness capabilities.

Gaps and incompleteness still remain, causing operational risks. These risks impede effectiveness and efficiency in achieving United States Government agency missions and stand as obstacles to achieving the NextGen vision to include the security of the aviation system, defense of the homeland, and the comprehensive transformation of the United States NAS.

A combination of newly developed, deployed, or planned procedures and technological advances for the NAS make NextGen goals attainable. The *Next Generation Air Transportation System's Integrated Plan* (2004) and *Next Generation Air Transportation System 2005 Progress Report* detail problems facing the NAS and identified six goals and 19 objectives to achieve the NextGen vision. The following objectives are particularly germane to this document:

- Reduce transit time and increase predictability
- Provide for common defense while minimizing civilian constraints
- Mitigate new and varied threats
- Ensure security efficiently serves demand
- Tailor strategies to threats, balancing costs and privacy issues
- Minimize impact of weather and other disruptions

The United States must continue to use the full range of its assets and capabilities to prevent the Air Domain from being used to commit acts of terrorism and other unlawful or hostile acts against the United States, its people, property, territory and allies and friends. The United States must strive to minimize the impact of its security interdiction efforts on the Aviation Transportation System (ATS)[6] and continue to facilitate the free flow and growth of trade and commerce in the Air Domain. These efforts are critical to global stability and economic growth, and are vital to United States interests.[7]

[5] Final Report of the Integrated Surveillance Study Team, October 31, 2008.

[6] National Security Presidential Directive (NSPD-47)/ Homeland Security Presidential Directive (HSPD-16), Aviation Security Policy, March 26, 2007.

[7] Ibid.

A guiding principle of NextGen is that safety and security of the NAS must be of primary concern: "Safety needs to be embedded at the core of all procedures, products, policies, or technologies associated with aviation."[8]

Further, a collaborative, cooperative approach among United States Government aviation security agencies is required to ensure coordinated planning for and response to threats in the Air Domain. This dual emphasis on safety and security means that completeness of sensor coverage to improve Air Domain situational awareness will be crucial to the success of integrated air surveillance.

Both the *National Strategy for Aviation Security (NSAS)* and the supporting *Air Domain Surveillance and Intelligence Integration (ADSII) Plan* offer guidance for improving Air Domain awareness: "To maximize domain awareness the Nation must have the ability to integrate surveillance data, all-source intelligence, law enforcement information and relevant open-source data from public and private sectors, including international partners."[9]

These documents provide that surveillance mission partners should synchronize surveillance efforts and integrate capabilities to monitor, detect, identify and track aerial objects persistently, within and outside of the United States.

Multiple departments and agencies require air surveillance and security data and information to satisfy often overlapping aviation-related roles and responsibilities. These organizations and their associated needs include:

1. Department of Transportation (DOT)/Federal Aviation Administration (FAA), for managing and regulating air traffic and supporting aviation security;
2. Department of Homeland Security (DHS), for coordinating the conduct of airborne and airport aviation security as part of a layered security construct, the investigation of criminal activities, regulatory violations and interdiction of suspect aircraft and orchestrating government efforts for emergency management;
3. Department of Defense (DoD), for executing Air Sovereignty and Air Defense missions and Civil Support for mitigating catastrophic events;
4. Office of the Director of National Intelligence (ODNI)/Intelligence Community for integrating surveillance data generated by Federal elements with its analyses to enabled prudent planning and crisis response capabilities;
5. Department of Commerce (DOC), for conducting surveillance in obtaining and providing atmospheric information to generate weather forecasts and information on routine and hazardous weather affecting ATS operations; and
6. Department of Justice (DOJ), for the investigation and prosecution of criminal activities, terrorist acts, or terrorist threats by individuals or groups inside the United States, or

[8] Department of Transportation and Joint Planning and Development Office. Next Generation Air Transportation System Integrated Plan, 2004. Available at: http://www. jpdo.gov/ library/NGATS_v1_1204r.pdf

[9] National Strategy for Aviation Security Air Domain Surveillance and Intelligence Integration: December 19, 2008

directed at United States citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States.

To maximize domain awareness, the United States Government will continue to invest in and improve enhanced sensor technology; Intelligence, Surveillance and Reconnaissance (ISR) capabilities; and information processing tools and training of analysts to monitor the NAS.[10] Improvements through the 2018 to 2025 timeframe should include effective monitoring of operating vehicles, terrorists, persons of interest, and aviation infrastructure in identified areas of interest, at designated times and provision of improved surveillance consistent with operational needs, benefits and cost. Over the next 14 years, air surveillance research, technology development and transfer, testing and evaluation should seek to provide a persistent capability for detecting and monitoring all types of airborne vehicles, in all weather conditions, in the required areas of coverage.[11]

1.1 Purpose

This interagency IS ConOps provides an operational foundation for the near term and long term integrated air surveillance mission. The near term is defined as the approval date of this document through 2018. Many of the capabilities described in this IS ConOps are achievable using non-materiel solutions (e.g., training, policy, cross-organizational coordination, etc.), which should be addressed in the near term. Most of the capabilities that require acquisitions of materiel solutions are, by necessity, longer term issues. The long term is defined as 2019 and beyond.

Note: *Capabilities that can, or should, be delivered in the near term are underlined throughout the document.*

The IS ConOps serves these primary objectives:

- Identify needed air surveillance capabilities (refer to *Appendices A and D* for requirements specificity)
- Identify potential changes in how air surveillance capabilities can be combined and information integrated with intelligence and other sources to realize shared awareness goals
- Identify information needed for a complementary ISEA that informs near- and long-term budget formulation for the 2025 and beyond time frame
- Provide insight for influencing other follow-on analytic requirements development and acquisition processes of stakeholder departments and agencies

In so doing, the IS ConOps addresses the following key issues:

[10] Department of Transportation and Joint Planning and Development Office. Next Generation Air Transportation System Integrated Plan, 2004. Available at: http://www. jpdo.gov/ library/NGATS_v1_1204r.pdf.

[11] Final Report of the Integrated Surveillance Study Team, October 31, 2008

- The importance of making decisions in the near term, based on operational direction and engineering analysis, to achieve the right mix of sensors for required coverage
- The types of air surveillance information provided by each agency
- Secured integration and sharing of air surveillance, intelligence, and other associated pertinent information required by agencies for domain awareness
- The need to establish necessary levels of reliability, availability, and accuracy for surveillance information, as determined by each organization

1.2 Background

The *National Security Presidential Directive 47/Homeland Security Directive 16, Aviation Security Policy,* March 26, 2007, the *National Strategy for Aviation Security* of March 26, 2007, and the *Air Domain Surveillance and Intelligence Integration* of December 19, 2008, all highlight the need for a collaborative, cooperative relationship among the surveillance mission partners in order to ensure "unity of effort" in planning for, and responding to, threats in the Air Domain. Senior-leader participants of the December 2008 Surveillance Summit asked the SPC to accept the role as interim governing authority for interagency coordination of air surveillance for a period of 18 months. In accepting, the SPC agreed to provide an oversight mechanism for interagency homeland air surveillance, operations, and requirements pending the larger interagency effort to establish an Air Domain governance construct that would be connected to the National Security Council/National Security Staff.

The December 2008 *Surveillance…Vision for the Future* summit provided a platform to address interagency governance and policy barriers, as outlined in the JPDO IS Study Team's (ISST) final report on NextGen.[12] An outcome of the summit's Senior Executive discussions was for JPDO to obtain SPC approval to accomplish three tasks by July 2010:

- Coordinate development of a concept of operations for interagency air surveillance;
- Coordinate development of an interagency integrated air surveillance EA and funding profile; and
- Identify existing and potential executive bodies to provide enduring interagency governance of air surveillance activities.

In fulfillment of these tasks, the JPDO established an interagency IS ConOps Integrated Process Team (IPT), comprised of representatives from DHS, DOT/FAA, ODNI, DoD, DOC, and the JPDO. The IPT was established to address recommendations from the ISST final report.

In July 2010, the SPC agreed that the recommended governance mechanism and work plan be put into action and that the IS ConOps be updated, with the specific intent of resolving the outstanding issues that had prevented total concurrence in draft version 3.0.

The ADA initiative is creating an ADA OpsCon document. This IS ConOps will complement the air surveillance aspect of that OpsCon.

[12] Senior Leader Invitation Letters, 27 October 2008, Signed by DHS S-2

1.3 Scope

This IS ConOps identifies how interagency integrated air surveillance and information management capabilities available in the near-term time frame will enhance existing capabilities of surveillance mission partners to perform their specific missions. It was informed by many documents, both classified and unclassified, which are cited in *Appendix A*: *References*, and in the *Appendix D: Surveillance Capability Parameters*. In addition, the IS ConOps contributes to a broader goal of increased air domain awareness and collaborative interagency decision-making, while bridging requirements for NextGen in 2025 and beyond.

Specifically, the IS ConOps addresses the following issues:

- In-flight operations, as they relate to air surveillance and its data and associated aviation security information
- Aggregation and dissemination of such information
- Data and information exchange requirements within the integrated air surveillance domain
- Use of weather technologies as they apply to the integrated air surveillance operational concepts
- Other areas sufficient to meet stakeholders' persistent surveillance needs
- Domestic Air Space, which is defined as air space that "overlies the continental land mass of the United States [to include Alaska] plus Hawaii and United States possessions"[13] and their approaches. For the purposes of this document, we refer to it as domestic air space or the homeland.

The IS ConOps **does not** attempt to perform the following:

- Provide analysis of current or future gaps in surveillance coverage, although gaps may persist or emerge in the long-term timeframe
- Consider new sensors that may be under development by individual agencies (although all cooperative and non-cooperative surveillance sensor capabilities currently in use are assumed to be available through the near-term)
- Address aircraft operating on the ground
- Address weather observing
- Provide detailed coverage of all processes associated with pre-flight information gathering or internal department and agency decision-making surrounding the use of surveillance information

[13] FAA Order : JO 7110.65T Effective Date: February 11, 2010

1.4 Justification for Changes

Today, operational information sharing among partner agencies depends largely on the telephone (i.e., the Domestic Events Network [DEN]). Interagency command centers lack a common air picture as a result of limited automated information sharing, networking, and data integration among agencies. Not all sensor output and processed sensor information, including air tracks, are available to all agency users for a variety of reasons (e.g., data quality and reliability concerns, technical incompatibility limitations, policy decisions). Other surveillance-related information is also inaccessible to many surveillance operators. Results of these limitations include:

- Inefficiencies through duplication of efforts
- Gaps in surveillance information available to agencies
- Gaps in surveillance coverage, which adversely impact the ability of agencies to accomplish their missions

To satisfy the demands of air traffic management, aviation security, law enforcement, and national defense, agencies must take greater advantage of existing surveillance and surveillance-related resources (e.g., sensors and information assets) and leverage them to the fullest extent possible.

1.5 Coordination with Other Domains

Operations must be supportive of cross-domain collaboration and integration. Air surveillance sensors and associated information-sharing capabilities must eventually be integrated with the capabilities and activities of other physical domains (e.g., maritime, land, and space). Integration will be necessary to support maritime interdictions, land-based activity, and space launches effectively. Since activities in the Air Domain may easily shift to the maritime or land domains, it is essential that hand-offs for continued monitoring between and among the domains be handled smoothly.

1.6 Governance

As a result of the September 11, 2001 terrorist attacks, the need for improvements to homeland air surveillance and information exchange capabilities has been clearly acknowledged. However, efforts to deploy advanced capabilities have been hindered by the lack of an interagency governance policy capable of coordinating requirements, development efforts, acquisition programs and fiscal responsibility across agencies.

Programs with national stature and spanning several agencies require effective and enduring governance mechanisms to coordinate requirements, budgeting, and execution among agencies. The governance structure for integrated air surveillance requires additional strength in the budgeting process to ensure that the Office of Management and Budget (OMB) and appropriate Congressional committees recognize and properly manage requirements and budgets that encompass multiple agencies. To this end, mindful of individual agency processes, the integrated air surveillance governance process must perform the following functions:

- Coordinate efforts and interests of policy-makers, regulatory authorities, and leaders from participating agencies
- Identify cross-agency requirements to aggregate national solutions on integrated surveillance capabilities
- Establish priorities
- Create a cross-agency air surveillance road map to synchronize agency surveillance initiatives
- Coordinate development and submission of complimentary agency budgets
- Facilitate and monitor execution of the above

Of specific importance to integrated air surveillance, the advent of Automatic Dependent Surveillance-Broadcast (ADS-B) as the primary means of cooperative surveillance for FAA Air Traffic Management operations stands out as a prime challenge. While the FAA has determined that it does not require primary long-range radar (LRR) coverage to support its mission, DoD and DHS will continue to rely heavily on these radars for their defense, security and law enforcement missions. By 2025-2030, the current service life extension program for these radars will end. If the program is not extended, or capabilities provided or replaced by other means, long-standing capability gaps will remain unresolved, which will be further compounded by widespread loss of non-cooperative surveillance in key areas. Clearly, each of the partner agencies has some requirement for non-cooperative surveillance. Identifying and documenting the extent of those requirements and accompanying responsibilities will require coordination and collaboration.

A challenge for integrated United States air surveillance stakeholders is to have the right policies, processes and resources in place for the integrated air surveillance mission. An analysis is needed to determine what resources will satisfy the stated requirements of all partner agencies and identify areas where requirements intersect. The results of the analysis will provide agencies with information they need to prioritize acquisition and development objectives and to share the cost of realizing those objectives in a manner that will benefit all parties.

The ISST Final Report addresses the critical importance of governance:

> There are many potential mechanisms that might be used to oversee Integrated Surveillance for NextGen. Given the complexity of the task and the different priorities of the surveillance mission partners, the ISST believes that any successful governance structure must be collaboratively developed by the White House and the Congress, to ensure alignment of responsibility, authority and funding…. [The ADAB has been established to] support development of the whole-of-government solution, [clarify] ADA priorities, and [synchronize] future interagency actions by identifying overarching investment goals and potential policy/strategic level synergies, redundancies, and conflicts[14].

Section 8 of this ConOps, *Recommendations,* lists initial recommended targets for an integrated air surveillance governance process.

[14] Air Domain Awareness Board Charter, [Approval Date]

2 Current Operations and Systems

This section provides a brief description of essential, present-day air domain surveillance operational elements for each agency bearing primary responsibility for homeland defense and the safety and security of the NAS: FAA, DoD, DOC, DHS, and ODNI, on behalf of the Intelligence Community. Sections 2.3 and 2.4 address operational and policy constraints that apply to current operations and systems.

2.1 Description of Current Operations

Air and atmospheric surveillance operations are conducted in support of national defense, security and law enforcement, air traffic management, and weather forecasting. An aircraft displaying suspicious behavior causes the agencies responsible for the safety, security, and defense of the homeland to determine which of these three mission areas the aircraft behavior falls under and then respond accordingly. Protection and safety of the homeland and its approaches are their essential responsibilities.

The United States Government operates over 400 land-based radars (long-range, terminal, and air defense) for North American surveillance coverage from the surface to approximately 60,000 feet above mean sea level (MSL). In some areas, the FAA uses cooperative surveillance systems to provide surveillance information while assuring aircraft separation.

Airborne and Tethered Aerostat Radar Systems (TARS) augment surveillance for DHS and DoD by providing additional low-level, “look-down” surveillance along United States borders and some capability in air approaches over the Caribbean. Additionally, DHS and DoD coordinate the deployment of ground mobile radars to counter emerging threats in the border environments. (In the Caribbean, DoD over-the-horizon radars are primarily tasked with conducting counter-narcotics missions.)

The Next Generation Weather Radar (NEXRAD) system maintained by the National Oceanic and Atmospheric Administration (NOAA) comprises 159 Weather Surveillance Radar-1988 Doppler (WSR-88D) sites throughout the United States and select overseas locations. This system is a joint effort of DOC, DoD, and DOT. In addition to the three meteorological base data quantities that these radars produce -- reflectivity, mean radial velocity, and spectrum width -computer processing generates numerous meteorological analysis products. Dual Polarization capability is currently being added to all WSR-88D units, with completion in 2013.

Other surveillance-related information resources, both inside and outside the continental United States include the United States Intelligence Community (IC) and foreign partners including Canada, the North Atlantic Treaty Organization (NATO), Mexico, and the European Organisation for the Safety of Air Navigation (EUROCONTROL). DoD integrates sensor data and other surveillance-related data at the North American Aerospace Defense Command (NORAD) air defense sectors. A number of DHS departments, including Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), United States Coast Guard (USCG), and United States Secret Service

(USSS) collect, analyze, integrate, and disseminate surveillance data and other information to support aviation safety and security.

Changing mission requirements of surveillance mission partners have resulted in a number of collaborative efforts to improve the delivery of surveillance capabilities. Several examples of these efforts include:

- FAA and United States Air Force (USAF) collaboration on radar Moving Target Detection technology
- DoD, DHS and FAA collaboration consider potential long and short term solutions for terminal and long range radars
- Joint development of the current surveillance architecture, in which cooperative and non-cooperative surveillance data are integrated at the sensor prior to dissemination
- A collaborative joint development and acquisition program to obtain new terminal radar data processing and air traffic control automation systems for FAA and DoD - Standard Terminal Automation Replacement System (STARS)
- DOC and FAA, with awareness and monitoring by DoD, examine the NEXRAD replacement, which may be capable of detecting weather and aircraft using the same sensor infrastructure

2.1.1 Federal Aviation Administration

The FAA's overarching mission is "to provide the safest, most efficient aerospace system in the world."[15] To this end, the FAA bears primary responsibility for regulating and providing air traffic separation, safety advisories, and other safety services to civil and military aircraft operating in the NAS as well as other Air Domain safety and security operations, including:

- Planning and implementing airspace restrictions and other air traffic management
- Providing separation assurance between air vehicles and between aircraft and terrain as well as restricted airspace
- Detecting, identifying, tracking, and monitoring NAS operations as a function of the provision of air traffic management services, including possible security incidents
- Reporting anomalies/non-conformance appropriately for determining security risk profiles
- Providing Air Traffic Management (ATM) services that support airborne operational threat response, including DoD and DHS efforts to detect and track aircraft for air sovereignty and air defense
- Sharing pre-flight and in-flight information, flight plan changes, Air Traffic Control (ATC) clearances, and other Air Domain information with surveillance mission partners

The FAA provides these essential functions, many involving labor-intensive, manual processes, which are related to air surveillance:

[15] FAA Mission: http://www.faa.gov/about/Mission/.

- Flight plan processing
- Flight monitoring
- Traffic control
- First Alerting
- Flight operations support
- NAS operations monitoring
- NAS usage planning

These functions require surveillance data in real time or recorded surveillance data for post analysis operations. The real time surveillance service provides air traffic state data for automation services, aircrews, air traffic personnel, and others, enabling shared situational awareness from which to conduct safe and expeditious air and surface operations. Recorded surveillance data is used for post-event analysis, airspace design, procedure design, and quality assurance/control. The FAA shares surveillance-related information with surveillance mission partners predominantly by manual and verbal coordination.

The FAA, in coordination with DoD and DHS, also provides NAS operations security in these core functions:

- Security policy development
- Early warning
- Security implementation for the NAS
- Coordination of security activities and issues
- Balancing security implementation against NAS air transportation needs

The FAA operates the DEN teleconference, which is used by all partners to identify, monitor, manage, and coordinate security situations as well as to conduct crisis response and emergency operations. A variety of coordination tools, aircraft situational displays, and security related databases with limited inter-connectivity support the DEN, but the teleconference is the primary means for sharing information.

2.1.2 Department of Defense

DoD executes its homeland defense responsibilities through NORAD, United States Northern Command (USNORTHCOM), and United States Pacific Command (USPACOM). These commands are responsible for preparation, planning, and response execution, including use of lethal force, in support of DoD missions.

DoD currently relies on FAA and joint FAA, DHS, and DoD cooperative and non-cooperative surveillance sensors and on alerts from air traffic controllers and DHS Air and Marine Operations Center (AMOC) detection enforcement officers, as primary sources of information about anomalous and suspicious activity in the NAS. In coordination with the FAA, DoD also operates DoD radars and conducts air traffic safety operations in those areas of the NAS airspace for which it is primarily responsible. DoD airborne surveillance aircraft, Tethered Aerostat Radar Systems, over-the-horizon radars and other ground-based radars provide additional air surveillance capability in critical border regions and other targeted areas. However, current data feeds from DoD and FAA surveillance systems are not uniformly integrated, and the exchange of other surveillance-related information among mission partners is predominantly conducted through manual processes and voice communications.

NORAD is assigned three missions through the NORAD Agreement: (1) aerospace warning; (2) aerospace control; and (3) maritime warning. Responsibilities under these three missions include:

- Deter, detect, and defend against aerospace threats to North America
- Provide timely, accurate integrated threat warning and attack assessment
- Provide timely, accurate maritime warning to North America

USNORTHCOM conducts homeland defense, civil support, and security cooperation to defend and secure the United States and its interests. Its primary responsibilities include:

- Monitoring Areas of Responsibility (AORs) that include air, land, and sea approaches and encompass the continental United States, Alaska, Canada, Mexico and the surrounding water out to approximately 500 nautical miles
- Planning, organizing, and executing homeland defense and civil support missions, as ordered by the President or Secretary of Defense
- Executing civil support missions that include domestic disaster relief operations (e.g. wildfires, hurricanes, floods and earthquakes.)

Support also includes counter-drug operations and managing the consequences of a terrorist event employing a weapon of mass destruction. The command provides assistance to a Primary Agency when tasked by the Secretary of Defense.

2.1.3 Department of Homeland Security

The National Strategy for Aviation Security describes detailed lead responsibilities for DHS in stating that it "will coordinate the operational implementation of the Strategy, including the integration and synchronization of related Federal programs and initiatives.[16] In support of this directive, DHS conducts air surveillance and Air Domain Awareness operations by coordinating law enforcement and other air assets to detect, intercept, interdict, and track cooperative and non-cooperative aircraft. Responsibilities include:

- Establish security risk criteria and determine operational security threats; and
- Detect, track, intercept, interdict, and conduct surveillance of cooperative and non-cooperative aircraft for coordinating the conduct of DHS air security mission activities and de-conflicting with simultaneous DoD air defense operations.

[16] National Strategy for Aviation Security, March 26, 2007

DHS air surveillance operations also depend heavily on accessing information from a wide range of intelligence, law enforcement, and open source databases, which today are largely incompatible. As a result, DHS operators conducting investigations must query separate databases for information as well as undertake extensive communications among the multiple DHS partner agencies to cue and coordinate air security law enforcement operations.

2.1.3.1 Customs and Border Protection

Customs and Border Protection (CBP) directs the AMOC, a multi-agency organization that coordinates the DHS effort to provide localized homeland air security during a National Special Security Event (NSSE) and border security operations to counter narcotics smuggling, human trafficking, and terrorism. To execute this effort, the AMOC's Air and Marine Operations Surveillance System (AMOSS) leverages multiple sensors and aggregates intelligence and information from law enforcement and open-source databases.

AMOC's current technologies allow AMOSS users to receive, integrate, and view sensor and track data from multiple sensors, such as:

- Ground and air-based radars
- Tethered Aerostat Radar Systems
- Optical sensors on Unmanned Aerial Vehicles (UAVs)
- Automatic Identification System (AIS) data
- Link-16 data link on-board aircraft
- Friendly Force Tracker (FFT) satellite tracking devices
- Airborne Early Warning (AEW) aircraft (e.g., P-3 with E-2 radar)

CBP, through the Office of Air and Marine, maintains a fleet of interceptor, utility and surveillance aircraft that support national and local domain awareness efforts by conducting intercepts, interdictions and surveillance in support of criminal investigations and response to disaster and recovery efforts.

2.1.3.2 Transportation Security Administration

Created by the Aviation and Transportation Security Act (ATSA), Public Law 107-71, on November 19, 2001, the TSA is the primary federal entity responsible for aviation security. Its primary responsibilities include:

- Receiving, assessing, and distributing intelligence information related to transportation security
- Assessing threats to transportation
- Developing policies, strategies, and plans for dealing with threats to transportation security
- Developing other plans related to transportation security, including coordinating countermeasures with appropriate departments, agencies, and instrumentalities of the United States Government

- Serving as primary liaison for transportation security to the intelligence and law enforcement communities
- Enforcing security-related regulations and requirements
- Working in conjunction with the FAA Administrator on any actions or activities that may affect aviation safety or air carrier operations
- Working with the International Civil Aviation Organization and appropriate aeronautic authorities of foreign governments under section 44907 of Title 49 of the United States Code to address security concerns on passenger flights by foreign air carriers in foreign air transportation
- Carrying out such other duties and exercising such other powers, relating to transportation security as the TSA Administrator considers appropriate, to the extent authorized by law.

To execute those responsibilities, the TSA established the Transportation Security Operations Center (TSOC) to serve as the centralized hub for collecting, assessing, and disseminating operational information for all transportation modes.

The TSOC collaborates with counterparts from FAA and other agencies to share information in real time and to coordinate response plans and actions. For example, during events involving a possible security threat, concern, or anomaly regarding one or more aircraft, the TSOC provides all pertinent available information that may bear upon the status, security, and recommended disposition of the aircraft in question.

As unresolved aviation security events may become air defense events, the TSOC is also responsible for collecting and disseminating relevant information such as:

- The presence of Federal Air Marshal Service (FAMS) teams on airliners
- The presence of armed Federal Flight Deck Officer(s) (FFDOs) in the cockpit or other armed law enforcement officers in the cabin
- Any screening anomalies noted at the departure airport
- Airline corporate office or owner of the airplane
- Aircraft's fuel load and estimated range/flight time
- Passenger and crew manifest information
- Presence of hazardous cargo

The TSOC is located within the TSA Freedom Center, which also hosts the National Capital Region Coordination Center (NCRCC). The NCRCC is an interagency-staffed organization whose coordinated actions are intended to enhance the effectiveness of air security and defense operations in the National Capital Region (NCR) and the restricted airspace around Camp David, Maryland.[17] The NCRCC also includes full-time 24/7 representation from the FAA, DoD, CBP, United States Coast Guard (USCG), United States Capitol Police and United States Secret Service (USSS).

[17] National Capital Region Coordination Center (NCRCC) Concept of Operations, April 2011.

To support the TSOC's and the NCRCC's requirements for air surveillance situation awareness and related agency responsibilities, the Freedom Center features several complementary air traffic and surveillance systems. Key among these are the CBP's Air Marine Operations Surveillance System (AMOSS), the DoD's Battle Control System - Fixed (BCS-F) Remote Tactical Air Picture (RTAP), the FAA's Enhanced Traffic Management System (ETMS), and the TSA-FAA Automatic Detection and Processing Terminal (ADAPT) V2. The ADAPT V2 system is particularly well suited to TSA's mission requirements because it combines the surveillance capabilities and user interface of AMOSS, with enhanced real-time cross-referencing against internal and external databases, including:

- All TSA Aircraft Operator Security Programs
- FAA-TSA Airspace Authorizations/Waivers
- State Department diplomatic clearances
- Stolen aircraft database
- European Union Banned / Restricted aircraft
- United States and Canadian aircraft registration data
- Airline and aircraft information
- Special Interest Flight (SIF) categories
- Official Airline Guide (OAG) information

2.1.3.3 United States Immigration and Customs Enforcement

United States Immigration and Customs Enforcement (ICE) is the primary investigative agency for smuggling acts committed in the air domain. ICE maintains close ties to the CBP Office of Air and Marine and is fully integrated into the AMOC staff, where ICE leads the Law Enforcement Division. ICE also maintains liaison officers at TSOC, JIATF-South, JIATF-West and the National Targeting Center-Passenger.

2.1.4 Department of Commerce

The National Oceanic and Atmospheric Administration (NOAA) mission is as follows:

- Understand and predict changes in climate, weather, oceans, and coasts
- Share that knowledge and information with others

As part of the interagency Air Domain surveillance team, NOAA provides weather information for shared situational awareness. NOAA utilizes the following resources to gather and distribute weather data:

- Satellite systems
- Weather radars
- Surface/upper air observing system
- Ships, buoys, aircraft, and research facilities
- High-performance computing with information management and distribution systems

NOAA also anticipates working with the IS partner agencies to explore the potential for obtaining weather information from air surveillance systems and for providing air surveillance information from NOAA weather radar systems.

2.1.5 Intelligence Community

The Intelligence Community (IC) gathers and exploits several types of intelligence:

- Geospatial Intelligence (GEOINT)
- Signals Intelligence (SIGINT)
- Human Intelligence (HUMINT)
- Measurement and Signature Intelligence (MASINT)
- Open Source Intelligence (OSINT)

In addition, the IC leverages information-sharing relationships with non-IC partners, such as law enforcement, regulatory, and other Federal agencies and public, private, industry, and allied partners, to assess and disseminate Air Domain-related information concerning:

- Groups or individuals with hostile intent
- Movement of dangerous or illicit cargo
- The state of worldwide aviation infrastructure

IC aviation security-associated responsibilities include:

- Conducting all-source analysis regarding terrorism, proliferation, narcotics, hostile nation-state, and illicit activity that threaten United States and allied nation interests in the Air Domain
- Identifying and analyzing threats to the Air Domain, complementing surveillance to detect actual threats if, and when, they materialize.
- Providing interagency partners, policymakers, and operators with the necessary insight to enable them to take appropriate preventive, defensive, or operational response measures;
- Providing timely, relevant, and accurate information on the worldwide aviation infrastructure
- Supporting response and recovery from an attack by contributing to identification of perpetrators; assessing tactics, techniques, and procedures to inform decisions about short- and long-term aviation security measures; and sharing analyses with those responsible for planning and operational actions
- Helping to identify and cue, based on intelligence reporting, portions of the air surveillance picture that are of national security interest
- Integrating air surveillance data generated by the FAA, CBP, DoD, and other elements with IC analyses to enable security planning and crisis response capabilities

The combined lack of integrated shared data and an “analysis architecture” from which a User Defined Operational Picture (UDOP) can be produced, constrains intelligence integration and information sharing within the IC and across the non-IC. This constraint hinders IC efforts to carry out its aviation security responsibilities. Net-centric capabilities and enterprise-wide service-oriented architectures can be used to support shared domain awareness in order to integrate interagency partners' capabilities. These capabilities align with ODNI's *Vision 2015* and presidential direction to maximize shared domain awareness in NSPD-47/HSPD-16.

2.2 Current System Characteristics

Figure 1 shows how air surveillance sources and systems are organized today. Surveillance sources (e.g., primary radar, secondary radar, Airborne Warning and Control System [AWACS], Automatic Dependent Surveillance [ADS]) provide data to government agency command and control (C2) systems. Multiple point-to-point and Internet Protocol (IP) networks connect sources where an ad hoc sharing architecture has evolved to distribute surveillance source information to different C2 centers. Such sharing has evolved along with joint radar development and usage agreements over time.

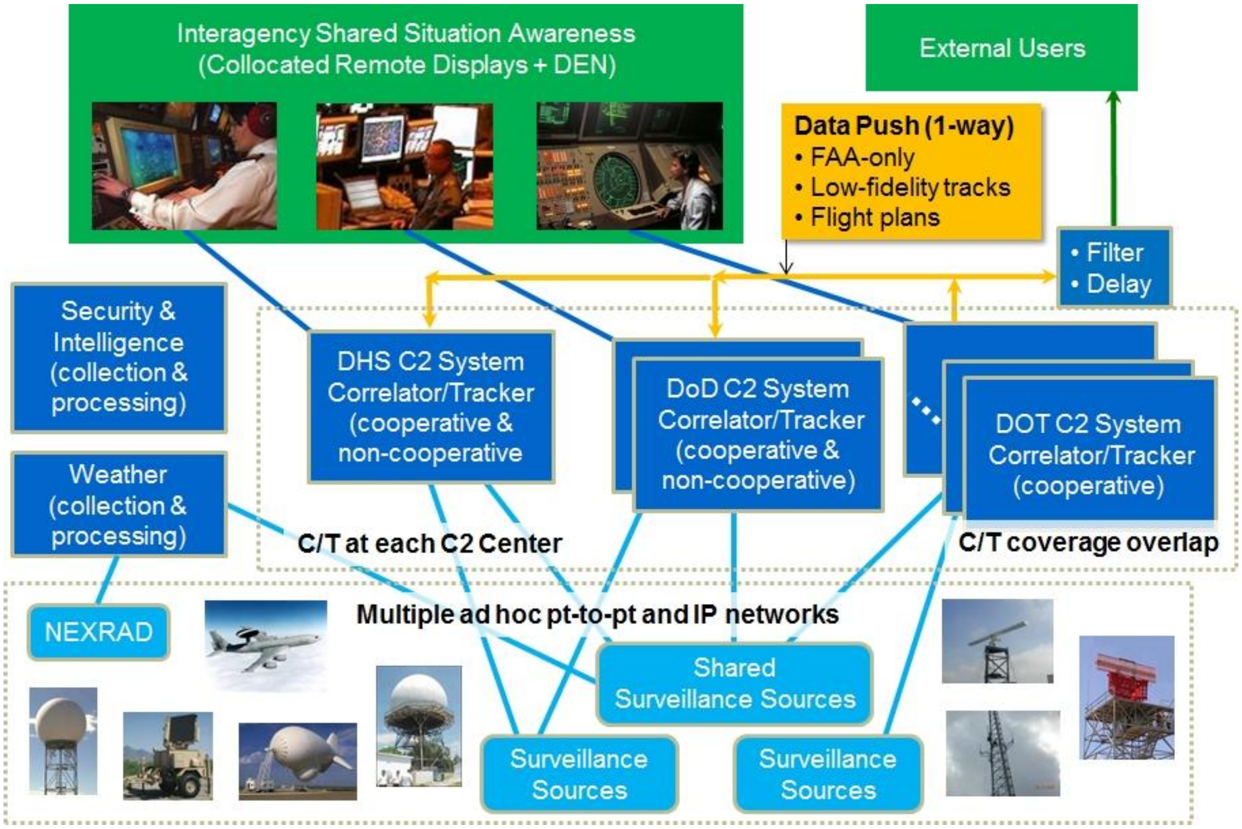
Interagency Shared Situation Awareness
(Collocated Remote Displays + DEN)
External Users
Data Push (1-way)
• FAA-only
• Low-fidelity tracks
• Flight plans
• Filter
• Delay
Security & Intelligence (collection & processing)
Weather (collection & processing)
DHS C2 System Correlator/Tracker (cooperative & non-cooperative
DoD C2 System Correlator/Tracker (cooperative & non-cooperative)
DOT C2 System Correlator/Tracker (cooperative)
C/T at each C2 Center
C/T coverage overlap
NEXRAD
Multiple ad hoc pt-to-pt and IP networks
Shared Surveillance Sources
Surveillance Sources
Surveillance Sources

Figure 1: NAS Surveillance Today

Each C2 center provides a correlator-tracker function that produces estimates of position, speed and ground track angle. Each center develops the correlator-tracker function to serve its own needs. FAA distributes track data for use by other government systems and external (commercial) interests serving the general public. The FAA also distributes flight plan and ATC clearance data for external users. Interagency Shared Situational Awareness is facilitated primarily by multiple teleconferences (including the DEN). Shared Situational Awareness (SSA) is improved further in the NCRCC by collocating disparate remote displays for DoD, DHS, and DOT C2 automation.

2.3 Operational Constraints

Current air surveillance operations and infrastructure are not integrated and automated across partner agencies. Information needed to assess the intent of an anomalous and/or suspiciously-behaving aircraft is not accessible to all partners across the multitude of their systems. The inability to acquire, fuse, and analyze disparate interagency data and information feeds automatically hinders detection, identification, tracking, and monitoring operations. For example, the FAA-operated DEN, which is used to conduct crisis response and emergency operations, relies primarily on voice communication as the primary source of interagency information. It lacks digital communications and coordination tools to support the DEN, as illustrated in Figure 2 below:

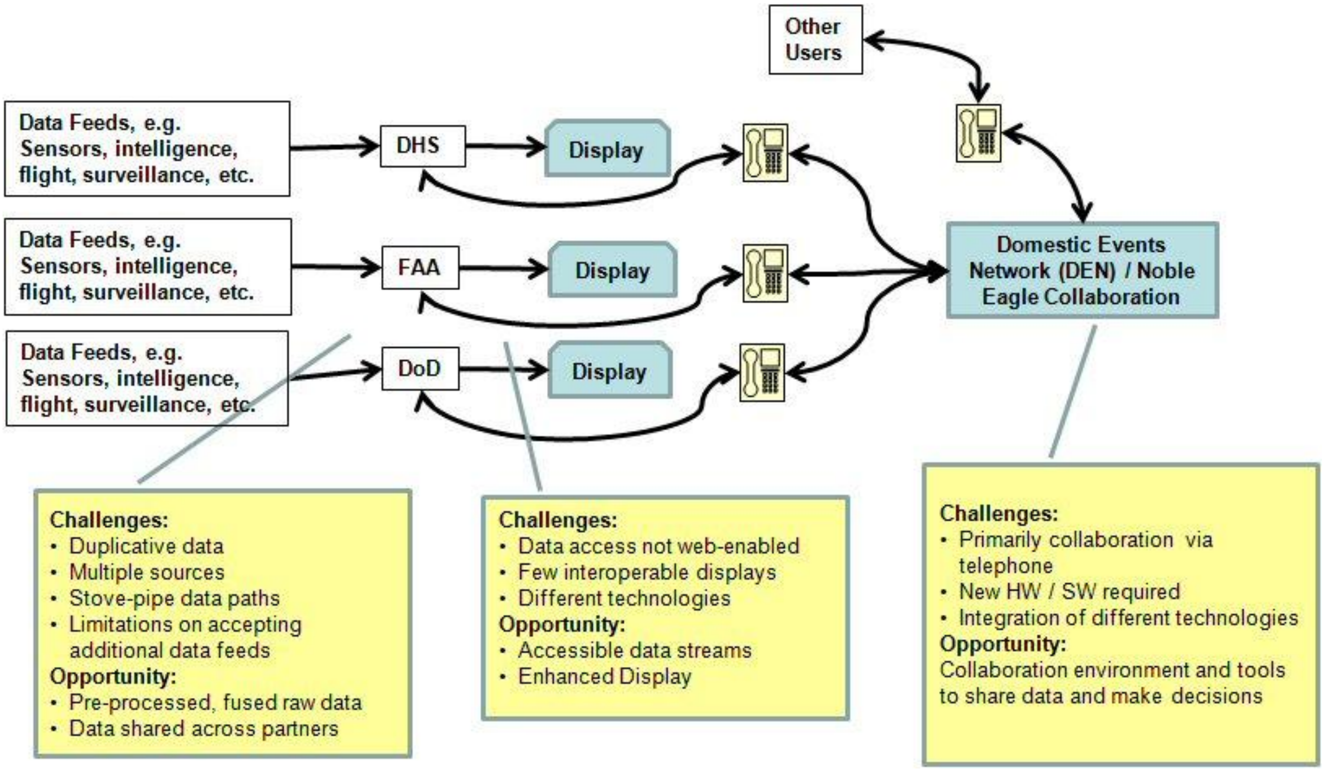
Other Users
Data Feeds, e.g. Sensors, intelligence, flight, surveillance, etc.
DHS
Display
Data Feeds, e.g. Sensors, intelligence, flight, surveillance, etc.
FAA
Display
Domestic Events Network (DEN) / Noble Eagle Collaboration
Data Feeds, e.g. Sensors, intelligence, flight, surveillance, etc.
DoD
Display
Challenges:
• Duplicative data
• Multiple sources
• Stove-pipe data paths
• Limitations on accepting additional data feeds
Opportunity:
• Pre-processed, fused raw data
• Data shared across partners
Challenges:
• Data access not web-enabled
• Few interoperable displays
• Different technologies
Opportunity:
• Accessible data streams
• Enhanced Display
Challenges:
• Primarily collaboration via telephone
• New HW / SW required
• Integration of different technologies
Opportunity:
Collaboration environment and tools to share data and make decisions

Figure 2: Current Integrated Air Surveillance Challenges

Shortfalls and gaps in current operations and systems, in addition to constraints on information sharing, limit broader shared situational awareness and the full leveraging of existing interagency air surveillance systems and capabilities. Gaps exist at low altitudes across most of the United States interior, as well as the oceanic approaches. Incomplete coverage and limited capabilities to conduct wide-area surveillance off the coasts produce additional gaps. Current plans to use legacy systems, which were designed for specific agencies and missions, attempt to improve coverage through information sharing. However, these plans will not improve completeness of coverage by sensors.

2.4 Policy Constraints

In order to achieve integrated air surveillance information sharing, integration, and automation objectives, the ADAB needs to inform policies relating to the integrated air surveillance domain aimed toward the following objectives:

- Support development, budgeting, and execution of multi-agency programs
- Address completeness of coverage based on an agreed-upon risk analysis
- Address cross-domain access to sensitive, restricted, or classified information, including access by surveillance mission partners during normal operations and by authorized law enforcement and other authorized users during contingency events
- Support implementation of an information-sharing infrastructure
- Refine integrated surveillance mission definitions to ensure no gaps in mission coverage, process, or decision-making
- Align integrated surveillance roles and responsibilities defined within the agency with those proposed from a multi-agency standpoint
- Define the multi-agency back-up sequence, cooperation, and response to ADS-B failure

3 Description of Desired Operational Capabilities

Integrated air surveillance services must be able to detect, monitor, track, and identify all air vehicles and atmospheric weather in and approaching the NAS. This capability will serve the purposes of air traffic management, aviation safety, air security, air defense, and law enforcement. As such, future integrated air surveillance services must meet growth in traffic demand and ensure protection from an increasing number of potential threats. These services include:

- Reduced separation spacing and a move towards all weather visual-equivalent operations to meet NextGen's goal of increased capacity for civil aviation
- An integrated User-Defined Operational Picture that provides capability to access flight information for any track of interest, across all partner agencies, as applicable security and need-to-know conditions permit
- Accurate, comprehensive, and readily accessible preflight information (e.g., flight plan intent, reliable pre-flight and in-flight risk assessments) that enables monitoring flight path conformance and determination of bona fide risks to aviation security
- Data from all surveillance sources, including cooperative and non-cooperative sensor systems, will be accessible and made available/exposed for operational display and data processing
- Integration of surveillance information from multiple sources, including classified systems, that provide real-time access to information needed to deter and prevent threats before they enter United States airspace
- Routine air traffic operations conducted in a manner that supports both increased air traffic and increased flight safety
- Key information exchanges automated and shared via the Net-Centric infrastructure, where feasible
- Implementation of NextGen key concept elements: management by trajectories, flight objects, net-centric operations, and facilities transformation
- Ability to integrate additional and emergent surveillance capabilities as they are developed
- Ability to integrate information from other domains such as maritime and land
- Ability to incorporate information from non- United States sources

3.1 Operational Policies and Principles

Sections 2.3 and 2.4 discussed current operational and policy constraints that impede air surveillance operations. Many of these will continue through the near-term and beyond. Nonetheless, the United States must address them in order to bring about the changes needed to achieve integrated air surveillance objectives. This section describes those changes.

The Air Domain Surveillance and Intelligence Integration Plan[18] specifically names detection and prevention, information sharing, and integration as guiding principles. These principles inform the near-term operational concepts for integrated air surveillance, which encompass the following:

- Informing, through aggregation of all available flight-related information
- Monitoring, in service of both air traffic safety and preserving security and defense of the homeland
- Detecting planned or actual anomalous and/or suspicious behavior within and approaching the NAS
- Identifying and locating safety and security threats to the Air Domain
- Assessing and responding to identified safety, security and defense threats

This unprecedented exchange of information across every level of government and between public and private sectors will require policy and legal changes. Rule-making concerning adoption of ADS-B by aircraft originating both inside and outside of the United States will have significant policy and operational implications for integrated air surveillance partners in the near-term and beyond. In anticipation of such changes, Section 710 of the Vision 100 - Century of Aviation Reauthorization Act (Public Law 108-176) directed DOT, DOC, DoD, DHS, the National Aeronautics and Space Administration (NASA), and the Office of Science & Technology Policy (OSTP) to work together in developing and implementing operations and technologies that bring about and support NextGen in accordance with pertinent policies, regulations, and legislation. ODNI was added as an “Ex Officio” member of the JPDO Senior Policy Committee and supporting Executive Board to support implementation of NextGen activities and facilitate the integration of surveillance and intelligence capabilities to enhance aviation security of United States interests worldwide.

3.2 Assumptions

For purposes of this IS ConOps, the following assumptions are critical to successful integrated air surveillance:

- The United States Government will establish an effective governance process that is capable of initiating and executing cross-agency initiatives.
- Existing non-cooperative surveillance sensors including FAA en route and terminal radars will not undergo changes in ownership, operation, or location, and they will need to remain in service beyond the near term if not replaced by an alternative.
- Current FAA terminal airspace approach radars will still be operational in the near-term. The FAA will transition from current transponder technology for en route and terminal surveillance to the ADS-B system (with the rule taking effect in 2020) as the primary method of handling commercial Instrument Flight Rules (IFR) traffic.

[18] White House. Air Domain Surveillance and Intelligence Integration Plan, March 2007. Available at: http://www.dhs.gov/xlibrary/assets/hspd16_domsurvintelplan.pdf

- Mission-level roles and responsibilities of partner agencies will remain as presently assigned, even if modifications to operational, system, and information exchange capabilities impact roles and responsibilities of system users at the tactical level.
- This IS ConOps applies only to surveillance of air vehicles in flight, not on the ground.
- This IS ConOps does not cover post-flight analysis and decision-making, or operational responses (i.e., post-flight agency execution/engagement activities).
- Intelligence will be available, as appropriate, to support and be integrated into aviation surveillance requirements.
- NOAA will continue to operate its current generation of weather surveillance sensors and will not field weather radars that can simultaneously track air vehicles with sufficient accuracy to complement air vehicle surveillance systems before the near term timeframe.
- NOAA is developing the initial version of the Four-Dimensional (4-D) Weather Data Cube for aviation weather data in support of the NextGen Program.
- DoD and DHS will continue to preserve and maintain existing long range radar capabilities, principally through execution of the long range radar service life extension program. As indications and warnings demand, or as operations require, DoD and DHS will employ tactical/mobile surveillance assets.
- Integration of FAA and international surveillance and flight data coverage of oceanic and international airspace will not change during the timeframe of this IS ConOps.
- Integrated Surveillance agency partners will support cooperative efforts to develop new surveillance technologies.

3.3 Constraints

Many current operational and policy constraints will continue throughout the near and long term time frames and even beyond, including the following:

- A dedicated governance mechanism is not yet in place for a national integrated air surveillance capability.
- The widespread exchange of information advocated by this IS ConOps, including gathering, analysis, and dissemination activities, must be conducted in compliance with the following:
  - Applicable laws
  - Executive Orders
  - Presidential Directives
  - Attorney General-approved guidelines
  - Federal Court orders/procedures
  - Respective Department/Agency policy and guidance
  - International arrangements and agreements regarding information sharing
- Policy changes and new interagency agreements will be required to implement information exchange activities.
- No existing network architecture exists for automated interagency processing, integration, and dissemination of information, between interagency networks or across different levels of classification, in such a way that ensures that such information is accessible only by those with appropriate clearance.

- Standards for the seamless exchange of information from multiple, incompatible sources, whether classified or not, have either not been developed or uniformly adopted.
- International agreements for net-centric information sharing have not been negotiated.

3.4 Integrated Air Surveillance Environment

For civil aviation, security, and defense operations, integrated air surveillance will be based on three fundamental principles:

- Maximize operational benefits for all mission partners
- Ensure safe, secure, and efficient operations in the NAS
- Harmonize global aviation to move passengers and cargo freely.

Integrated air surveillance operates within an environment of information sharing, cooperative and non-cooperative surveillance, location-specific operations, and unmanned aircraft systems operations as described in the following sub-sections.

3.4.1 Information Sharing Operations

Enabling technologies will provide interagency Shared Situational Awareness through an enterprise network that distributes surveillance source, track, and geographic data for use by external systems and government C2 facilities that provide air traffic management, security, defense, and other services. Such technologies include:

- Net-Centric sharing of data and information
- Shared services that process source data
- Selected exchange protocols that distribute information

Shared sources include:

- Fixed site, mobile, and air-based
- Surface, upper air, satellite, and weather radar sensors
- ADS services

Weather information will be provided through the 4-D Weather Data Cube and the single authoritative source capabilities as described in the NextGen Weather ConOps. While the DoD will leverage and populate the 4-D Weather Data Cube, DoD-unique weather requirements will be met through the appropriate DoD Services' weather forecasters and forecasting systems.

The long term, high-level concept for information sharing shown in Figure 3 below is based on establishment of a Net-Centric Information Sharing Environment that enables organizations with integrated surveillance mission responsibilities to discover and share information as they need it. While this vision may not be fully achieved within the near-term, it does establish a framework for designing, programming and acquiring the needed capabilities described in this IS ConOps.

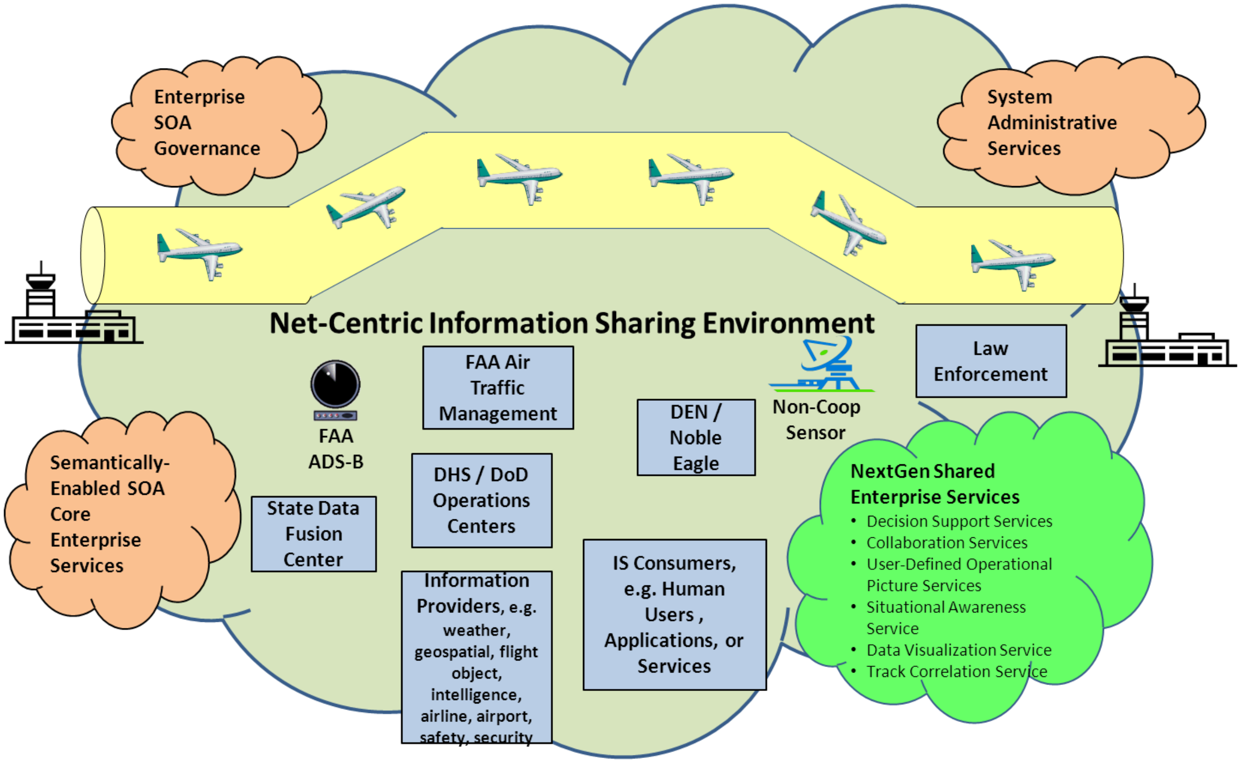
Enterprise SOA Governance
System Administrative Services
Net-Centric Information Sharing Environment
FAA Air Traffic Management
Law Enforcement
FAA ADS-B
DEN / Noble Eagle
Non-Coop Sensor
Semantically-Enabled SOA Core Enterprise Services
DHS / DoD Operations Centers
State Data Fusion Center
NextGen Shared Enterprise Services
Decision Support Services
Collaboration Services
User-Defined Operational Picture Services
Situational Awareness Service
Data Visualization Service
Track Correlation Service
IS Consumers, e.g. Human Users, Applications, or Services
Information Providers, e.g. weather, geospatial, flight object, intelligence, airline, airport, safety, security

Figure 3: NextGen Integrated Air Surveillance High-Level Information Sharing Concept

The Net-Centric information-sharing environment enables data collection and collaboration among operations centers, IS information consumers, Noble Eagle conference members, law enforcement and other integrated surveillance partners.

All partners will have access to data from information providers (e.g., sensor data, weather, flight object, Information Sharing Environment-Suspicious Activity Report [ISE-SAR], critical infrastructure, geospatial imagery, terrain, and map information). Participants will also have access to a set of NextGen shared enterprise services, e.g., decision support, collaboration, situational awareness, and data visualization to support accomplishment of their missions.

Shared data is correlated, combined, and enhanced by common shared situation awareness trackers and mission-specific trackers, and other data reduction processes and then augmented with mission-specific data (e.g., air vehicle flight plans, clearances, weather watch areas, analysis results and interpretation).

3.4.2 Surveillance Operations

Cooperative surveillance operations using ADS-B surveillance information will enhance existing radar-based surveillance information used for ATC automation functions such as tracking, minimum safe altitude warning (MSAW) and conflict alerting. ADS-B-enhanced cockpit displays will enable flight crews to see positions of other aircraft on the ground, in-flight, and in final approach, thereby reducing potential for deviations, errors, and collisions. For example, NAS users equipped with ADS-B avionics will be better able to maintain separation from other aircraft, even when visibility is reduced, and will be able to detect potential conflict, in some cases even before ATC detects it. In addition, air traffic management operations will benefit from increased efficiency based on optimal spacing intervals between aircraft.

Non-cooperative surveillance sensors do not require transponders and will assist cooperative surveillance sensors in detecting and identifying objects. This type of surveillance is required for defense, security, and law enforcement missions. It is also required for ATC in high-density terminal areas and must complement other ATC needs when the required cooperative surveillance capability is lost.

Additional sources of non-surveillance information will be shared among interagency partners supporting DOT, DoD, DOC, and DHS missions. Examples of this type of data include, flight risk profile data, payload information (e.g., flight crew, passengers, or cargo), aircraft owner/operator information, intelligence, weather data, and other situational awareness-related information.

3.4.3 Location-Specific Operations

This section of the IS ConOps describes how surveillance operations differ by location and situation. Drawing distinctions in surveillance realms can highlight how differences in airspace management and control rules, proximity to critical infrastructure and key resources (CI/KR), and availability of information, affect agency interdiction and air traffic management decisions. These distinctions inform subsequent decisions about whether or where to place new sensors by identifying levels of domain awareness that can be achieved using expected near-term capabilities in different locations and situations and with respect to different classes of air vehicles.

3.4.3.1 Approach from outside by unauthorized flights

Agreements between Canada and the United States , and between Mexico and the United States , for sharing surveillance sensor data, track histories, flight plans, and aircraft and crew profiles through net-centric information-sharing systems will be an important component in United States efforts to protect the homeland. In event of an unauthorized air approach from outside the NAS, shared surveillance track data from Canada and Mexico will provide United States security and defense partners with timely information needed to locate, identify, track, and respond to the aircraft. Should interdiction be necessary, integration of surveillance information, including data from NAV Canada and from the Mexican Director General of Civil Aeronautics (DGAC), will provide operators with a more complete picture from which to inform decision makers and direct actions.

Equally important to Air Domain protection is the ability of interagency surveillance partners to prevent unauthorized approaches from outside the United States before they occur. In the NextGen environment, pre-flight information will be available to enable assessment of risks, based on information known before the flight launches.

3.4.3.2 Cities and critical infrastructure

Improved surveillance information-sharing capabilities in the near term will facilitate increased safety in ATM operations and protection of cities, critical infrastructure and other key assets located inside the United States and its territories. NextGen will support automation to reduce flight separation standards and increase airspace capacity through user-executed airborne spacing, sequencing, and separation operations. NextGen will enable automatic messages to appropriate agencies, in the event of a breach or impending breach of volumetric boundaries surrounding cities and other key assets, whether or not offending flights fall within pre-established, reportable risk profile criteria.

Such messages will provide sufficient time and information for surveillance mission partners to assess the magnitude of threats and to decide upon and execute an appropriate response in far less time and with far more available information than today. NextGen's track data and information-sharing capabilities will allow agencies to track and assess flights of interest collaboratively. Same track monitoring will also provide agencies tasked with coordinating and carrying out interdictions with an enhanced picture of threat locations and status and the locations and status of responding friendly aircraft.

3.4.3.3 Open range flight

For less populated and more remote areas within the United States , current fiscal limitations prevent the same level of surveillance sensor density that exists in more densely populated urban environments. This situation will continue through the near-term. Additionally, in these areas, more Visual Flight Rules (VFR) traffic operates with little or no interaction with ATM operators. In the near-term, there will be little change in the persistent surveillance capabilities in these areas. However, enhanced data sharing and net-centric operations will allow incorporation of available existing sensors and mobile sensors to develop capabilities around critical infrastructure and key resources in the areas as needed.

General aviation (GA) aircraft equipped with ADS-B avionics will have a significant advantage at regional airports with limited radar coverage. Currently, such airports use labor-intensive timed-approach procedures, thereby limiting the number of aircraft that can make an approach even in favorable weather conditions. Significant delays are common for arrivals and departures in inclement weather. Increased ADS-B service at selected locations will enable ATC to provide radar-like flight separation services at these airports with significant benefits to NAS users.

GA aircraft in open range flight pose a different risk than that of commercial aircraft around large cities. As in present day operations, surveillance mission partners in the near-term will not have the same level of pre-flight knowledge about GA flights that they have for commercial aircraft because many GA aircraft do not file flight plans, and the percentage of GA aircraft outfitted with ADS-B will be significantly less than the percentage of commercial aircraft outfitted with ADS-B.

While some GA aircraft do not file flight plans and may not be fitted with ADS-B equipment, these aircraft tend to be smaller in size and pose a lower risk due to limited consequence if used in an attack. In the near term, it is possible for civilian infrastructure in open range areas to be highly vulnerable to attacks from the air. Additionally, threats may originate from open range areas thereby exposing a vulnerability to an attack in urban areas with more sensor coverage. Existing non-cooperative surveillance systems will continue to provide security and defense partners with crucial data in the near term. NextGen air surveillance improvements in the near-term, which are focused on improving information aggregation capabilities and overall situational awareness, will provide an opportunity to make a well-informed assessment of the numbers and types of surveillance sensors that will be required in open range airspace.

3.4.3.4 Temporary restrictions

Temporarily restricted airspace presents unique challenges to Air Domain safety and security. Surveillance capabilities are largely the same for temporarily restricted zones as they are for fixed sites. In the latter, however, surveillance mission partners have pre-established measures in place to facilitate effective monitoring of those zones. Permanent security volumetric expressions surround cities and critical infrastructure, which correlate flight risk levels with proximity to the asset. These expressions enable NAS automated services to ensure that a flight plan does not call for the aircraft to venture closer to a high-value asset than the flight's risk level warrants and to revise the flight trajectory, if appropriate.

Such automated calculations are not always available for temporary restrictions. The earlier a notice can be provided about a temporary restriction, the more partners will be able to replicate needed surveillance capabilities. National Special Security Events usually allow months of planning. Presidential visits are usually announced a few days in advance. In short notice situations, it may be difficult to ensure that everyone who needs to know about a Temporary Flight Restriction (TFR) receives notice. Inadvertent airspace penetrations are not uncommon in such circumstances, especially by aircraft flying VFR, which are not necessarily hostile, but merely uninformed. In these circumstances, agencies can only respond with whatever capabilities they have at their immediate disposal. The challenge is exacerbated in the situation where terrorists may strive to pass as a legitimate flight for as long as possible.

Improved information-sharing capabilities, intelligence aggregation services and automated alert capabilities will mitigate this problem to some extent. Information about aircraft and pilots, for instance, which are identified as higher-risk, can be quickly and widely disseminated to regional airports and other local officials. Automated alerts on aircraft exhibiting anomalous behavior can be sent as soon as the behavior occurs, thus increasing the window of time in which to respond to those aircraft.

3.4.4 Unmanned Aircraft Systems (UAS) Operations

<u>In the near-term, UAS must be able to operate as an integrated part of the NAS. A growing number and mix of UAS with varying capabilities and conducting operations at various altitudes and geographic locations will present significant operational and regulatory implications. For example, because UAS have no person onboard the aircraft, other capabilities such as onboard equipage, sensor (radar) tracking, or direct human observation must substitute.</u>

Air surveillance operations considerations regarding UAS operations will include the following:

- UAS operations will significantly increase within the NAS and in the approaches.
- UAS could provide additional air surveillance capabilities for integration into the mix of surveillance capabilities.
- UASs may be another node of data sharing capability, just as they are used in overseas operations today.

3.5 Desired Operational Capabilities

In the near term, air surveillance sensor data and other pertinent information will be provided by individual partners but jointly used by multiple partners. To maintain the safety and security of our national airspace and protect our nation from attacks originating from outside as well as from within the NAS, the data and information collection done by individual agencies will need to be complemented by automated capabilities for jointly accessing, viewing, analyzing, and sharing that information among all o mission partners. Every air surveillance partner should have the ability to contribute to, access, analyze, and share surveillance data and surveillance-related information in accordance with pre-established authorizations. Acquisition and development decisions made in the near-term must be aimed at providing complete coverage for the airspace within and approaching United States borders.

Achieving these capabilities will require cross-agency coordination for several purposes:

- Make decisions in the near-term that provide more complete sensor coverage for the NAS - inward and outward relative to the border.
- Capitalize on less costly and more readily-achievable goals of rapid coordination and information exchange among partner departments and agencies, which enable fulfillment of individual and interagency integrated air surveillance, safety, security, and defense responsibilities.
- Enable partners to improve the probability of discovering suspicious activity earlier and differentiating between aircraft experiencing navigational or procedural errors (including airspace violations) from those exhibiting hostile intent.
- Integrate air surveillance information and potential threat-related intelligence in order to provide accessible Air Domain safety and security information to all air safety, security, defense, and intelligence partners requiring such information.
- Maximize coordination between multi-agency air traffic, security, and defense operations to enable partners to detect, monitor, assess, sort, identify, deter, and take tactical action to mitigate threats to the homeland and to facilitate and manage airspace used for transportation and commerce.

Automated processing of information will complement current labor-intensive, time-consuming verbal or written communications. Automation of routine and common exchanges of information will supplement voice-only communications, providing improved data-capture, which will reduce the need for repetition and reduce the possibilities for miscommunication. For

<u>example, manual data integration through repetitive querying of multiple, incompatible databases will be a thing of the past.</u>

Automation will not only accelerate surveillance mission partners' decision-making processes but will increase levels of confidence in decisions. Shared, automated and immediate access to all pertinent pre-flight information and continuous, real-time aggregation, and correlation of data feeds from surveillance systems will likewise provide DoD and DHS with information needed to make an accurate assessment of any given flight's security risk.

<u>The operational capabilities described in this section assume the existence of an effective governance process that coordinates and aligns operational capability requirements across the community.</u>

3.5.1 Confirmation of the same track

Air domain surveillance applies electronic and data processing technology to produce timely air traffic position and movement (ground speed and flight track) information supporting defense, homeland security, and safe and efficient air transportation missions. DoD, DHS, and FAA own and operate legacy surveillance sensors, data communications networks, and surveillance data processing systems that have evolved over time to satisfy changing mission needs.

Flight tracks are displayed differently on these legacy systems. In many cases, Integrated Surveillance partner agencies must collaborate in identifying, assessing, and responding to an anomalous flight. The different C2 systems used by different agencies each generate their own distinct tracks from the data they receive from primary, long range radars. Even though two C2 systems may be monitoring the same aircraft and receiving the same sensor inputs, the tracks that represent that aircraft are distinct in the two systems. Collaboration among geographically dispersed operators monitoring different C2 systems requires that they confirm that System A's track and System B's track indeed represent the same aircraft. Currently, voice communication among the operators is the only means of performing the confirmation, and this constraint sometimes imposes significant time delays on operators.

The NextGen Integrated Surveillance capability to provide confirmation of the same track will improve the identification process by making coordination with NextGen partners faster and more accurate. Information normally obtained by a phone call after an aircraft is designated as a pending, track of interest (TOI) or suspect track would be made available to surveillance operators on all systems using NextGen automated information-sharing capabilities.

3.5.2 Known pre-flight information will be shared before aircraft take off

Selected available pre-departure information (e.g., flight plans, aircraft, and crew-related data) will be gathered and shared between the FAA and DHS to provide the opportunity to determine whether or not a flight meets acceptable safety and risk standards. Automated and semi-automated systems will collect, aggregate, and disseminate this information so that risk profiles can be ready and accessible within a very short time after the FAA receives the flight plan. FAA and DHS analyses of the raw inputs received through NAS automation services will be automatically disseminated to appropriate Air Domain security partners and accessible to other partners as necessary and authorized. The establishment of procedures and protocols to gather and disseminate this information before flight will require the concerted efforts of policy-makers, legislators, regulatory authorities, and leaders from each participating agency.

Various types of pre-flight information will be processed through automated information collection and dissemination services for different classes of aircraft. In the case of commercial passenger aircraft, the aircraft type and tail number, call sign, flight plan, passenger flight risks and watch lists, as well as the anticipated presence or absence of Federal Air Marshals on board the aircraft, will all be collected and disseminated to FAA and DHS personnel pre-flight. The information and DHS Risk Profiles will also be accessible, as necessary, to other authorized air security partners and system users. This level of information will usually not be available for general aviation flights.

3.5.3 Increased track-monitoring confidence and user-defined operating picture

Authorized mission partners will have ready access to networked surveillance data and information from multiple, heretofore incompatible data sources, which will enable operators to select and display data on-demand as circumstances require.

3.5.4 Selected dissemination of updated in-flight information

New in-flight information that becomes available will be made available to appropriate recipients. Where feasible, such information will be updated and shared automatically. Examples include flight plan deviations, squawk changes, lost communications, lost radios and/or transponders, changes in aircraft, performance characteristics (autopilot on/off, throttle settings, attitude, etc.), passenger disturbances, presence of a Federal Air Marshal (FAM), evidence of an un-secure cockpit, threat information, National Capital Region and State Department waivers, and information about when the aircraft was last in foreign airspace. This dissemination capability will be tied to the UDOP capability, described in 3.5.3 above.

3.5.5 Improved Detection Capability

The ability to detect air vehicles of all sizes, traveling at varying altitudes and speeds, is crucial to effective air surveillance. Because threats to the homeland are continually evolving, air surveillance systems must be flexible and adaptable and able to detect new threats as they emerge. C2 and other sensor surveillance data processing systems must have access to data from all available means, including all cooperative and non-cooperative surveillance sensors, to perform composite tracking, sensor integration and other state-of-the-art data-processing procedures that will produce the most accurate, high-quality, and comprehensive air picture possible.

3.5.6 Flexible sensor infrastructures

Operational and employment concepts should consider interagency requirements in the development and acquisition of sensors and infrastructure, which includes scalable and agile systems that provide certain flexibility:

- Rapid reconfiguration to detect targets that are outside the sensor’s normal use (e.g., using weather radar to detect air vehicle targets)
- Relocation to provide coverage in gap areas or to back-up installed sensors in a continuity of operations situation.

3.5.7 Agile information-sharing capability

Integrated air surveillance operations collect, aggregate, analyze, and disseminate data from surveillance sensors, as well as such information as flight plans, aircraft and crew profiles, risk profiles, and intelligence. Surveillance provides knowledge of current position, track history, and movement rate for vehicles in the Air Domain, while the other aviation-related information provides the context needed to create a comprehensive and shared picture of the NAS. This integrated picture provides robust and thorough aviation system situational awareness to support routine air traffic operations and off-nominal operations involving anomalous or suspicious activity. This integration will also provide the foundation to conduct analyses and interpretations.

The information-sharing capability must be agile to accommodate changes in threats, evolution of technology, and expanded mission requirements. It must allow cross-domain access to sensitive, restricted, or classified information, including access by authorized law enforcement and other users. Further, it must be able to mitigate failures among its components and networks (e.g., decreased system performance and degradation of ADS-B).

4 Desired System Capabilities

Section 3 of this document described the desired operational capabilities that support achievement of integrated air surveillance goals and objectives. This section describes the desired system capabilities that support those operational capabilities.

The NextGen Information Sharing Environment (ISE) diagram shown in Figure 4 below illustrates an environment where a set of technical architecture, standards, and profiles provides a mechanism to achieve broad-based information sharing across the aviation community. The goal is to use the technical standards and profiles to drive procurements that require common system interfaces within a Service-Oriented Architecture (SOA). These common interfaces will enable achievement of the NextGen and integrated air surveillance interoperability and information sharing objectives.

These technical standards and profiles can be targeted for incorporation into procurements as performance specifications for system acquisitions.

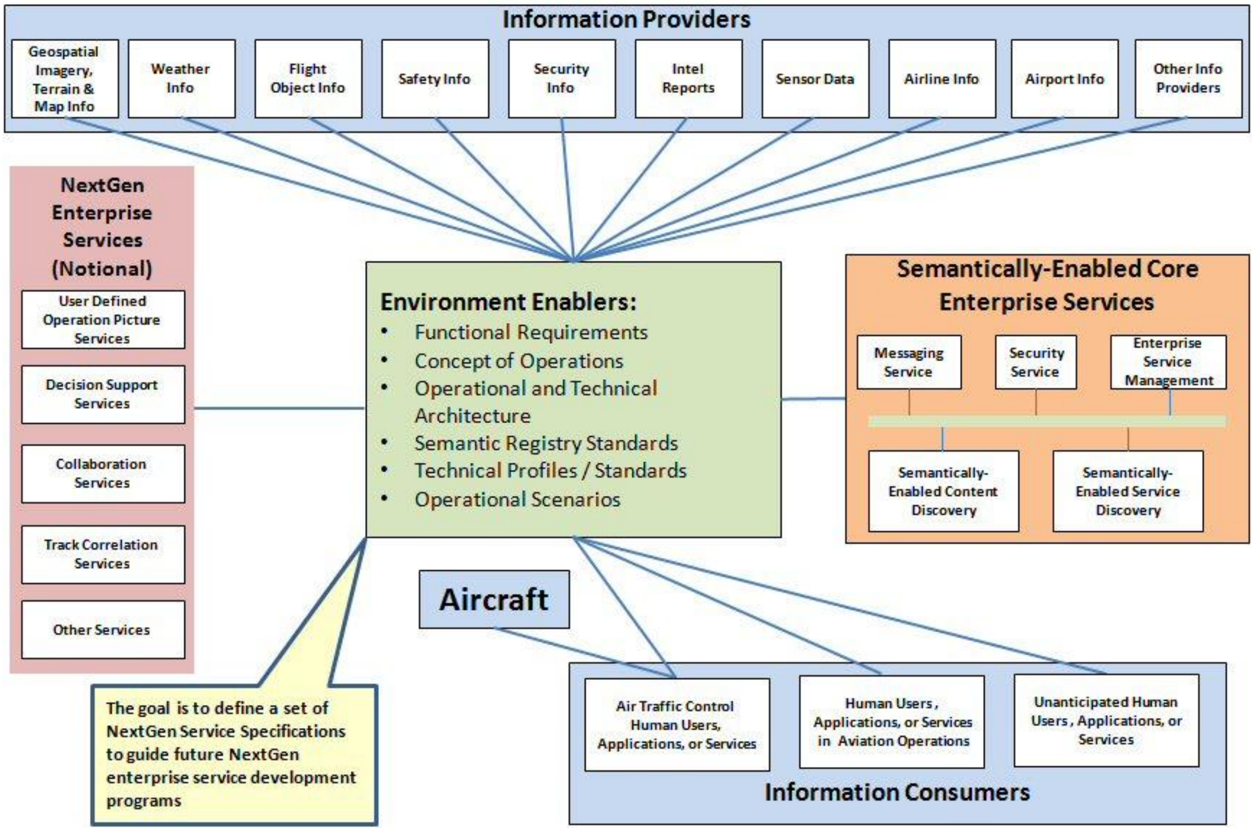
Information Providers
Geospatial Imagery, Terrain & Map Info
Weather Info
Flight Object Info
Safety Info
Security Info
Intel Reports
Sensor Data
Airline Info
Airport Info
Other Info Providers
NextGen Enterprise Services (Notional)
User Defined Operation Picture Services
Decision Support Services
Collaboration Services
Track Correlation Services
Other Services
Environment Enablers:
Functional Requirements
Concept of Operations
Operational and Technical Architecture
Semantic Registry Standards
Technical Profiles / Standards
Operational Scenarios
Semantically-Enabled Core Enterprise Services
Messaging Service
Security Service
Enterprise Service Management
Semantically-Enabled Content Discovery
Semantically-Enabled Service Discovery
Aircraft
The goal is to define a set of NextGen Service Specifications to guide future NextGen enterprise service development programs
Air Traffic Control Human Users, Applications, or Services
Human Users, Applications, or Services in Aviation Operations
Unanticipated Human Users, Applications, or Services
Information Consumers

Figure 4: NextGen Information Sharing Environment Description

4.1 Interagency Detection and Maintenance of Tracks

Integrated air surveillance systems must provide the capability to detect and maintain tracks in such a manner that two or more individuals, at different agencies, or within the same agency, monitoring separate watch screens, can quickly confirm when the tracks they are looking at on their respective screens represent the same object.

4.2 Agile Information Sharing Infrastructure

4.2.1 Surveillance Information Sharing Capabilities

An integrated information-sharing environment will enable distribution and sharing of information from data collection systems, such as radar, multilateration, ADS, and national intelligence capabilities. Data from these sources will be correlated and processed to produce position and velocity information for air vehicles.

Track surveillance reports of air vehicles will be linked over time, enabling a continuous record of movement as well as real-time position and continuity of associated information. Automated processes will apply appropriate security and privacy policies to track data and manage source data distribution.

Information will be available for use by automated operator decision support functions and the Air Domain situation displays to enable operational coordination among government agencies in addition to supporting routine services and tasks.

4.2.2 Cooperative and Non-Cooperative Means

Surveillance systems will require sources (e.g., sensors and systems) able to obtain position information using cooperative and non-cooperative means for detecting aircraft.

4.2.3 Use of Non-Surveillance Data

IS systems should be capable of sharing non-surveillance data associated with surveillance tracks, as appropriate, among interagency partners supporting DOT, DoD, DOC, and DHS missions. Examples of this type of data include, flight risk profile data, payload information (e.g., flight crew, passengers or cargo), aircraft owner/operator information, intelligence, weather data, and other situational awareness-related information.

4.2.4 Shared Services

Automated processing of sensor and other surveillance information will occur through shared services, accessible through an enterprise network infrastructure, that provide for collecting, correlating, tracking, fusing, data reduction and management of airborne vehicle position and movement data. However, more general services will also be provided, such as information discovery and translation. The IS architecture effort will identify specific shared services. Shared services include:

- Data management
- Track correlation
- Intelligence capabilities
- Association of intelligence with surveillance tracks
- Weather data reduction

4.2.5 Enterprise Network

A Net-Centric infrastructure will distribute appropriately protected information between and among shared services, command centers, and individual users. This network will have applicable class-of-service attributes, quality-of-service attributes, and communications protocols for delivery of the type of information available through shared services.

Shared interagency architectures will describe an economical national surveillance service, including cost and performance benefits, that can be gained by using all available resources (e.g., systems and sensors) to satisfy integrated air surveillance goals and objectives. These resources will achieve required coverage and will be engineered to provide service availability and other Required Surveillance Performance (RSP) metrics that satisfy individual and combined agency requirements.

Fundamental enabling technologies for integrated air surveillance services include:

- Net-Centric data-distribution capability
- Service-oriented architecture implementation
- Air surveillance data-exchange protocols

4.2.6 Multi-Domain Environment

The agile information sharing infrastructure that supports the integrated surveillance mission is expected to encompass multiple different domains, each of which may be controlled and administered by different organizational entities, and which may operate at different levels of security classification (as defined in *Executive Order 13526*). To allow information sharing to occur in this environment, the agile information-sharing infrastructure will include:

- Network boundary protection mechanisms that allow information exchanges to occur among different domains at the same level of classification
- Cross-domain security gateways that enable automated passing and interagency sharing and collaboration of approved formatted information exchanges, such as track information, via accredited cross domain devices through varying classifications of information systems.

4.2.7 Information System Security Controls

Each of the domains within the agile information-sharing infrastructure will include information system security controls to support mission assurance for the domain, and to further provide integrity, confidentiality, and availability as needed within the domain, as described in *NIST 800-53, Recommended Security Controls for Federal Information Systems and Organizations*, and equivalent Federal guidance pertinent to the security level of the domain.[19] Controls used in different domains must be interoperable and harmonized at the appropriate points to allow the necessary sharing of information end-to-end. Access to information must be based on appropriate processes, such as attribute-based access controls (ABAC) and proper identification authentication, providing the proper information to the authorized user.

4.2.8 Quality of Shared Information

Requirements concerning the quality of data used for the integrated air surveillance mission will depend on purposes for which the data is being used. For example, data used in providing safety-of-life critical services, such as air traffic operations and weapons targeting, will have stringent requirements for availability and timeliness. The components of the agile information-sharing infrastructure must be designed, tested, and operated in order to provide the necessary performance and availability to meet these requirements where needed.

The information sharing infrastructure will also provide support for higher-level requirements related to information quality, such as:

- *Provenance* - An information receiver may need to be able to determine and authenticate the original data source and chain of custody of subsequent processing of the data;
- *Consistency* - Algorithms for processing and analyzing data may need to meet standards for consistency among mission partners (e.g., tracker, coordinate system, adaptation) to allow for shared situational awareness and collaborative decision making;
- *Accuracy* - Systems may have requirements for the maximum allowable error between the data values and the actual value of the quantity being measured; and
- *Data update rate* - Systems may impose requirements on the maximum time interval between new information updates.

4.2.9 Geo-Coordinated Data

Surveillance data distributed for shared use at different operations centers will be position-referenced using a common global coordinate system. Data may be converted to a local position reference system if operationally necessary.

4.3 Sensor Network

An information-sharing environment will deliver appropriately secured sensor data to facilities for subsequent automated processing. This network will have applicable class-of-service attributes, quality-of-service attributes, and communications protocols for delivery of near real

[19] National Institute of Standards and Technology (NIST) Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations, 2009.

time data. Partner agencies will network existing Federal surveillance sensors currently not in the network in order to take maximum advantage of their collective capabilities. Near-term shared surveillance capabilities include:

- Radar Coverage (Refer to Appendix A, References, and Appendix D, Surveillance Capability Parameters, for more specificity in requirements)
    - Border coverage
    - Terminal coverage
    - En Route coverage
- Radar Detection Capabilities
    - Low, slow, small-radar cross-section aircraft
    - High-altitude, supersonic aircraft
- Radar Use
    - Weather
    - Flight tracking
    - ATC – certified for safety
    - Target control – quality certification

- Non-cooperative and cooperative surveillance and Automatic Dependent Surveillance Services.

Sensor networks will be designed to mitigate the effects of the following:

- Interference from physical objects (e.g., wind farms, in-band emissions both intentional and unintentional)
- Commercial and governmental competition for bandwidth, frequency spectrum, or technologies
- Non-traditional relationships with atypical IS partners (e.g., Department of Energy for resolution of wind farm interference)
- Competition for frequency spectrum

Long term shared surveillance capabilities, defined in this IS ConOps as those that will be delivered 2019 and beyond, require acquisitions of materiel solutions. These acquisitions should provide desired completeness of coverage inside the United States NAS based upon an agreed upon risk analysis. As noted in the ISST Final Report: "The end state of surveillance integration should be a NextGen surveillance capability that can persistently detect/track operating air vehicles 24/7/365 in all weather conditions, on airport surfaces and from near the ground to near space."[20]

Sensors and systems used to detect air vehicles may be dedicated solely to that purpose or may be used for other purposes (e.g., use of primary radar to detect aircraft and meteorological phenomena), thereby lowering costs for the combined services.

[20] Final Report of the Integrated Surveillance Study Team, October 31, 2008, p.11.

The surveillance architecture should enable rapid reconfiguration of mobile assets to support contingency or unanticipated needs for equipment, with the explicit understanding that existing systems are acceptable, in order to meet the following requirements:

- Facilitate continuity of operations (COOP) after loss of access to a normal facility or after loss of equipment; and
- Respond to the need for a temporary command center or for coverage expansion/enhancement.

Reconfiguration alternatives should enable use of existing spare or portable equipment to include portable temporary systems as well as airborne systems. In contingency situations certain system limitations are acceptable (e.g., lower Required Surveillance Performance (RSP) standards may be acceptable).

4.4 Command Center Data Processing and Visual Displays

Command centers contain the processing, displays, automation, and people that use air surveillance information. UDOP capabilities will provide for shared situation awareness based on multiple data sets by the shared services. Command centers will process mission-specific data, e.g., analysis of air vehicle flight plans, clearances, intelligence information, and weather watch areas, which will complement shared services from other sources. They will also have the ability to publish and subscribe to specific track and geographic Air Domain information.

4.5 Cross Domain Security Gateways

Secure information-sharing capabilities will leverage gateway/data guard capabilities between different networks with multi-level security classifications. These capabilities will enable automated passing and interagency sharing and collaboration of varying classifications of information.

5 System Operation and Sustainment

5.1 Surveillance Performance Reporting

Surveillance systems should monitor and report real-time achieved surveillance performance (by coverage volumes) that will inform and enable operators to adapt when nominal RSP is unavailable. For example, air traffic managers may have to adjust planned traffic flow patterns or curtail specific operational capabilities for service volumes operating with degraded mode surveillance performance, as described below.

5.2 Full Required Surveillance Performance (RSP) and Modes of Operation

Surveillance systems should operate in nominal modes achieving full RSP and in degraded modes that support operations possible under a lower RSP. This capability enables a service in which the cost of high availability may be reduced in selected service volumes, yet also enables a system that provides usable surveillance capability when system disruptions affect service availability.

<u>The near-term air surveillance system will need to operate in a variety of modes:</u>

- *Nominal mode:* System services and functions are available and/or operational, depending upon the implementation segment.
- *Off-nominal mode:* System services and functions are not available and/or operational, depending upon the implementation segment. Additional services and functions might be operational in this case, depending on the nature of the off-nominal condition.
- *Degraded mode:* The system must be able to provide some reduced level of capability when sensors, digital components, communication links, etc., are degraded due to natural or manmade causes. In addition, the system must be robust enough to provide a reduced level of service when facilities are damaged.
- *Augmented mode:* The system must have the capability to augment the normal mode of operation with additional capability when special circumstance require. This augmented mode will also serve to mitigate degradation due to loss of facilities.
- *Exercise mode:* The system must have the capability for injection of exercise scenarios to train operators, supervisors, and managers in a realistic operational environment without degradation to the system.
- *Training mode:* The system must have a capability to train and refresh operators without degradation to the system.
- *Simultaneous operational mode:* In normal mode, the system must support operations in multiple modes (e.g., exercise mode and training mode) simultaneously without degradation to the system.

5.3 System Support

As a “system of systems”, integrated surveillance requires a cohesive interagency system support strategy that aligns with responsibilities such as may be envisioned by the ADAB governance process. This strategy needs to address cross-agency allocation of responsibilities for the following:

- Maintenance
- Supply
- Support and test equipment
- Manpower and personnel
- Training and training aids
- Technical data
- Computer resource support
- Packaging, handling, storage and transportation
- Facilities

The strategy also needs to consider interagency operations and interagency system interactions. For example, it needs to recognize that agencies execute missions across many different operations centers. Hence, an end-to-end, cross-agency approach will be needed.

6 Operational Scenarios

Operational scenarios provide a means for IS ConOps developers to translate operational concepts and descriptions into Enterprise Architecture (EA) views and roadmaps. They serve as representative exemplars of typical situations that occur in the integrated surveillance operational domain. In this regard, the following scenario abstracts portray concepts that provide varying details of operational descriptions ranging from an off-nominal to a more complex "Lost Cargo Jet" scenario. These scenarios are available at on the JPDO Joint Planning Environment: http://jpe.jpdo.gov/ee/request/home.

In all scenario abstracts listed below, incorporation of weather information into the shared situational awareness is a prerequisite for successful performance of the activity.

6.1 Tracking of lost cargo airliner within Continental United States (CONUS)

Scenario description: This scenario provides an operational view of risks imposed by suspicious activity relative to a large cargo aircraft (GA originated) and those activities associated with applying integrated surveillance concepts. It describes the interaction of FAA, DHS, and DoD organizations as they conduct their national security missions.

6.2 Fast Business Jet Penetration from Northern Border

Scenario description: This scenario introduces the risk of fast and potentially chartered aircraft that are generally well-equipped. . It demonstrates how surveillance information and Air Domain awareness capabilities are employed to detect and evaluate the intentions of unauthorized foreign aircraft penetrating the United States NAS from the Northern Border, including coordination and information sharing with Canada's air traffic management and defense authorities. The scenario emphasizes the necessity for timely operations and decision making that relies on integrated surveillance information.

6.3 Fast Business Jet Penetration from Gulf of Mexico

Scenario description: This scenario introduces the risk of fast and potentially chartered aircraft that are generally well-equipped and emphasizes the necessity for timely operations and decision making that rely on integrated surveillance information. It demonstrates how surveillance information and Air Domain awareness capabilities are employed to detect and evaluate the intentions of foreign aircraft penetrating the United States NAS from the Gulf of Mexico, including coordination and information sharing with Mexican air traffic control authorities.

6.4 Degraded Mode Automatic Dependent Surveillance-Broadcast (ADS-B)

Scenario description: ADS-B service is currently available and will increasingly be an important part of IS. This scenario, therefore, deals with how to mitigate an ADS-B loss and demonstrates how a commercial aircraft will utilize avionics, automation and other decision support tools to collaborate with the ANSP during a loss of the Global Navigation Satellite System signal. Operational collaboration remains sufficiently resilient to avoid a complete NAS degradation or shutdown.

6.5 Lost Pilot “Blunders” into Controlled Airspace

Scenario description: Many situations involving integrated surveillance require a decision at some point on whether a law-abiding pilot is performing in an unexpected manner or intending to commit a criminal act. This scenario demonstrates operational activities that occur when a non-cooperative target enters controlled airspace without non-cooperative surveillance coverage. It describes activities of the Air Navigation Service Provider (ANSP), which becomes aware of an aircraft not providing cooperative surveillance messages and operating in controlled airspace without authorization. In this scenario, the pilot is a law-abiding citizen who is contacted via the emergency radio channel and directed out of controlled airspace while other aircraft are diverted from the approach.

6.6 Off-Nominal General Aviation Flight

Scenario description: This operational scenario demonstrates how surveillance information and Air Domain awareness capabilities are employed to detect and determine the intent of criminal activity within the NAS. This scenario describes activities of the AMOC, the Air Navigation Service Provider Security Operations personnel, and local law enforcement as they attempt to identify and determine the intent of an anomalous flight in the NAS. Intelligence indicators, associated with the aircraft, indicate that the flight is operated by a drug cartel.

7 Summary of Impacts

7.1 Summary of Operational Impacts

Adoption of the desired operational and system capabilities described in Sections 3 and 4 of this IS ConOps will have far-reaching effects. Increased use of integrated sensors and net-centric information-sharing capabilities of integrated air surveillance systems will increase the safety, capacity, and efficiency of routine air traffic management and enable DoD and DHS to locate and identify commercial and general aviation aircraft more quickly and more effectively. Shared situational awareness will be greatly improved between stakeholders, facilities, NAS users and the FAA.

Automated-data and information-sharing capabilities in the near term should provide the following:

- Prompt identification of the same track; and for legally authorized agencies, immediate access to intelligence and other information pertaining to flights, their crews, passengers, cargo, and possible threat associations
- Aircraft type and tail number, supplemented by any information about the aircraft’s history, flight plans, and presence of Federal Air Marshals and potentially suspicious persons on board the aircraft can impact the risk level associated with any given flight
- Ready access to information from diverse sources will aid surveillance partners in achieving the most robust possible situational awareness in the shortest possible time, thereby enabling better, more timely decisions when dealing with both routine and anomalous air transportation activities
- Near real-time information gathered through newly automated information-sharing capabilities

Collectively, these capabilities will enable more accurate and timely decisions with less risk. No longer will the opening minutes of a DEN conference have to be spent with each agency trying to identify which track on its watch screen is the same track that appears on the watch screens of the other agencies. No exchanges of rudimentary information about the flight will be required to bring surveillance mission partners up-to-speed on the unfolding situation, as that information will have been accessible and/or disseminated automatically to everyone with a need to know.

Watch screens can be tailored by individual operators to reduce clutter by displaying only requested information, thereby allowing users to monitor suspicious and/or unknown tracks quickly and confidently. Conversely, watch personnel can be confident that basic changes in a flight’s status, particularly changes in security status, will be automatically updated and widely disseminated, even if the flight track was previously removed from the screen. Automated alerts concerning changes in a flight’s security will lessen the need for visual confirmation that an aircraft has left the bounds of its flight trajectory. Operations personnel will thus not only start from a higher level of shared situational awareness, but they will not be overly burdened by the information overload that can arise from having to sort and monitor all tracks manually. The operational result of this will be more timely response decisions.

Finally, automated information gathering and dissemination capabilities will provide vastly more accurate and complete data records and will support improved analytics such as post-event analysis. This capability can also prevent legal challenges related to the chain of custody of evidence, improving the chances for successful prosecution by law enforcement agencies of criminal acts and enforcement of air traffic control regulations.

7.2 Other Potential Impacts

7.2.1 Regulatory Impacts

The wide-spread sharing of information that NextGen air surveillance systems will engender has significant impacts for policy-making and for regulatory authorities that must ensure that information gathering, analysis, and dissemination activities are conducted in compliance with the following:

- Applicable laws
- Executive Orders
- Presidential Directives
- Attorney General-approved guidelines
- Federal Court orders/procedures
- Respective Department/Agency policy and guidance
- International arrangements and agreements regarding information sharing

7.2.2 Fiscal Impacts

Implementing the system-wide changes in the way air surveillance information is collected and disseminated will require a collaborative interagency approach and substantial investment.

7.2.3 Organizational Impacts:

As desired operational and system capabilities are widely adopted, additional impacts will occur:

- Innovative and unanticipated uses for and applications of the capabilities will be identified
- Organizational roles and missions will evolve to accommodate new information-sharing paradigms, which will necessitate the need for updated policy guidance
- New training and education regimens will be adopted
- The mix of personnel assigned to the surveillance mission area and the facilities in which they operate could change
- The collaborative decision-making environment engendered by these new capabilities will demand leaders with a more collaborative leadership skill set than the classic directive model of leadership

7.2.4 Acquisition Impacts:

Materiel solutions will be needed to bring the desired operational and system capabilities to fruition and in their wake, as related systems and sensors are developed and deployed, to complete the eventual national surveillance environment.

8 Recommendations

The following recommendations discuss efforts that are necessary for successful implementation of this IS ConOps. The effectiveness of the high-level integrated surveillance concepts described within this document hinge on establishment of an enduring governance mechanism that drives forward integrated air surveillance as a holistic national capability.

8.2 Governance

Recommendation: It is recommended that the Air Domain Awareness Board (ADAB) address the topics in this section.

Discussion: The integrated air surveillance concepts and capabilities described within this document are based on a series of foundational decisions and technologies that are appropriate for the ADAB to address as listed below, in recommended priority sequence:

- Cross-agency sensor infrastructure development and consolidation:
    - Determine the whole of government sensor mix needed (i.e., joint requirements development).
    - Perform cross agency acquisition, research, and development.
    - Perform cross agency maintenance, infusion of technology, and management
    - Ensure that cost sharing is planned into the process.
    - Ensure that interference mitigation actions are incorporated into sensor designs
- Shared information services across the surveillance community:
    - Implement a service to distribute FAA flight data to authorized users in the IS community.
    - Implement a service to distribute Suspicious Activity Report (SAR) data to authorized users in the IS community.
    - Implement a service to provide automated threat alarm, warning, and notification data to authorized users in the IS community.
- Net-Centric infrastructure:
    - Develop a cross-agency, Net-Centric architecture that describes an information-sharing infrastructure and its relationship to agency systems and services.
    - Provide a road map for implementing and managing a NextGen-managed Net-Centric network and services.
    - Set standards for cross-agency interoperability specifications.
- Improvements in multi-layer security (i.e., common policy across agencies)

8.3 Policy and Guidance Changes

Recommendation: It is recommended that the ADAB review and analyze, and as required, initiate and recommend changes in policies, directives, rules, and interagency agreements to support integrated air surveillance objectives with an initial focus on policies cited in this section and in Section 3.1 of this integrated air surveillance Concept of Operations.

Discussion: Shortfalls and gaps in current operations and systems, in addition to constraints on information sharing, limit broader shared situational awareness and the full leveraging of existing interagency air surveillance systems and capabilities. In order to improve operational policies and address existing policy constraints to improve surveillance coverage and facilitate information sharing, the ADAB needs to inform policies that relate to the integrated air surveillance domain.

9 Conclusion

Impacts on the near term national suite of sensors resulting from this IS ConOps will be limited by programs already in the acquisition pipeline and already planned increases in surveillance sensor networking. Nevertheless, they are still noteworthy. Decisions on sensor infrastructure should consider strengthening and widening the border coverage and expansion from the border looking inward and outward. Ultimately this expansion will increase coverage inside the United States and along its borders.

Integration of data from all available sensors, whether owned by FAA, DHS, DoD, or other agencies, will provide Air Domain surveillance partners with the most complete possible position and movement information inside the national airspace and its approaches. The benefits of having such an enhanced view of the airspace will include a greater chance of successful interdictions, when such responses are necessary and a lower likelihood of unintended impacts, as security and defense partners are able to detect, identify, and assess threats with a higher degree of precision and confidence.

Finally, the benefits of increasing of interagency surveillance information-sharing capabilities will allow the Federal government to be better informed as it makes decisions regarding which surveillance sensors to develop and deploy and where they need to be positioned. This approach should lower development and acquisition costs as well as result in a more effective and efficient, integrated sensor network.

Appendix A: References

1. Integrated Surveillance for the Next Generation Air Transportation System: Final Report of the Integrated Surveillance Study Team, October 31, 2008.

2. Federal Aviation Administration. Air Traffic Organization (ATO) Concept of Operations for Air Domain Security, Final Version 1.0, July 28, 2008.

3. Federal Aviation Administration. NextGen Implementation Plan, 2009.

4. Department of Transportation and Joint Planning and Development Office. NextGen Enterprise Architecture Fiscal Year (FY) 11, 2008.

5. Department of Transportation and Joint Planning and Development Office. Next Generation Air Transportation System Integrated Plan, 2004. Available at: http://www. jpdo.gov/library/NGATS_v1_1204r.pdf.

6. Next Generation Air Transportation System, Integrated Work Plan: A Functional Outline, Version 1.0, September 30, 2008.

7. National Airspace System Surveillance and Broadcast Services Concept of Operations, Version 4.0, May, 2008.

8. Security Annex Concept of Operations for the Next Generation Air Transportation System, Version 2.0, June 13, 2007.

9. National Strategy for Aviation Security (NSAS) Air Domain Surveillance and Intelligence Integration (ADSII): Action Item 102, Final v1.20, December 19, 2008

10. National Strategy for Aviation Security (NSAS) Air Domain Security Integration and Intelligence Supporting Plan: Action Item 103, July 15, 2008.

11. Department of Transportation and Joint Planning and Development Office. Concept of Operations for the Next Generation Air Transportation System, Version 2.0, June 13, 2007. Available at: http://www.jpdo.gov/library/NextGen_v2.0.pdf.

12. Department of Commerce and Office of the Federal Coordinator for Meteorology (OFCM). Working Group for Multifunction Phased Array Radar, Multifunction Phased Array Radar, 2008.

13. Department of Defense. Department of Defense Dictionary of Military and Associated Terms, 2001. Available at: http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

14. North American Aerospace Surveillance Council. North American Air Surveillance Plan, 2002.

15. Gordon, P., Moore, J., Park, J., & Richardson, H. (2007). Economic impacts of a terrorist attack on the UNITED STATES commercial aviation system study. *Risk Analysis, 27,* 3.

16. Joint NEO Spiral 1 Team. Network Enabled Operations (NEO) Spiral 1, Final Report, Boeing, 2008.

17. National Academy of Sciences, National Research Council and Committee on the Evaluation of the Multifunction Phased Array Radar Planning Process. Evaluation of the Multifunction Phased Array Radar Planning Process, 2008. Available at: http://www.nap.edu/catalog/12438.html.

18. President George W. Bush. National Security Presidential Directive/NSPD-47, Homeland Security Presidential Directive/HSPD-16, Aviation Security Policy, June 20, 2006.

19. Vision 100-Century of Aviation Reauthorization Act. Public Law 108-176. *United States Statutes at Large.* 117 Stat. 2490.

20. White House. Air Domain Surveillance and Intelligence Integration Plan, March 2007 and Aviation Operational Threat Response Plan, March 2007. Available at: http://www.

dhs.gov/xlibrary/assets/hspd16_domsurvintelplan.pdf and http://www.dhs.gov/xlibrary/assets/hspd16_opthreatrespplan.pdf.

21. White House. Aviation Transportation System Security Plan, March 2007. Available at: http://www.dhs.gov/xlibrary/assets/hspd16_transsystemsecurityplan.pdf.

22. White House. Domestic Outreach Plan, March 2007. Available at: http://www.dhs.gov/xlibrary/assets/hspd16_domoutreachplan.pdf.

23. White House. International Outreach Plan, March 2007. Available at: http://www.dhs.gov/xlibrary/assets/hspd16_intloutreachplan.pdf.

24. White House. National Strategy for Aviation Security, March 2007. Available at: http://www.whitehouse.gov/homeland/nstrategy_asecurity.pdf.

25. Federal Aviation Administration. Crisis Management Handbook, November 2003.

26. Domestic Events Network Customer Guide Version 4, ATO Systems Operations Security, June 1, 2007.

27. Federal Aviation Administration Order 1900.1G, FAA Emergency Operations Plan, September 11, 2006.

28. Federal Aviation Administration Order 1910.1J, Continuity of Operations Plan for Washington Headquarters, July 6, 2006.

29. Federal Aviation Administration Order 7110.65, Air Traffic Control, February 16, 2006.

30. Federal Aviation Administration Order 7210.3, Facility Operation and Administration, February 19, 2004.

31. Homeland Security Presidential Directive (HSPD-1), Organization of the Homeland Security Council, October 29, 2001.

32. Homeland Security Presidential Directive (HSPD-5), Management of Domestic Incidents, February 28, 2003.

33. Department of Defense and Federal Aviation Administration Joint Order 7610.4M, Special Operations, January 18, 2007.

34. Department of Homeland Security. National Response Framework, January 2008

35. National Security Presidential Directive (NSPD-47)/ Homeland Security Presidential Directive (HSPD-16), Aviation Security Policy, March 26, 2007.

36. Federal Aviation Administration, NAS-SR-1000, National Airspace System Requirements Specification.

37. United States Code Title 49–Transportation, 2004.

38. Concept of Use for the Automated Data Analysis and Processing Terminal (ADAPT).

39. National Airspace System Enterprise Architecture, Operational Improvements and Mid-term Scenarios.

40. National Airspace System Surveillance and Broadcast Services Concept of Operations Version 1.0, May 11, 2006.

41. CRS Report for Congress, Securing General Aviation, January 24, 2008.

42. NSPD-47/HSPD-16, June 20, 2006.

43. Air Domain Surveillance and Intelligence Integration (ADSII) Plan, Mar 26, 2007.

44. Interagency MANPADS Concept Plan (CONPLAN), March 3, 2009.

45. United States Intelligence Activities, Executive Order 12333, as amended.

46. National Security Act of 1947, 50 U.S.C. 40, (July 26, 1947), as amended by the Intelligence Reform and Terrorism Protection Act of 2004, Public Law 108-458.

47. Terrorism, 18 U.S.C., Chapter 113B, § 2332(a), 2332(g) and 921, as amended by the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458.

48. Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, 2004.
49. Director of National Intelligence Vision 2015: A Globally Networked and Integrated Intelligence Enterprise.
50. Intelligence Community Directive 902, Global Maritime and Air Intelligence Integration, January 14, 2009.
51. North American Air Surveillance Plan (NAASP), Interagency Operational Requirements and Initial Funding Profile, October 23, 2002.
52. Plan for the Emergency Security Control of Air Traffic (ESCAT), Federal Register Vol 71 No. 203, 32 CFR Part 245, October 20, 2006.
53. ADSII Supporting Plan Action Item 93, Shared Criteria for Tracks of Interest, June 27, 2007.
54. ADSII Supporting Plan Action Items 95 and 98, Recommendation for Development and Implementation of Automation Systems in Support of NSAS, February 25, 2008.
55. ADSII Supporting Plan Action Item 96, Recommendation for Development and Implementation of Automation Systems in Support of NSAS, February 25, 2008.
56. National Strategy for Aviation Security (NSAS) Air Domain Surveillance and Intelligence Integration (ADSII): Action Item 102, Final v1.20, December 19, 2008.
57. National Strategy for Aviation Security (NSAS) Air Domain Security Integration and Intelligence Supporting Plan: Action Item 103, July 15, 2008.
58. Aviation Operational Threat Response (AOTR) Supporting Plan, AOTR Protocols, September 2007.
59. AOTR Supporting Plan Action Item 60, July 24, 2008.
60. AOTR Supporting Plan Action Item 61, Documentation of the Procedures to Coordinate the Decision and Execution of Diverting Tracks of Interest (TOI), July 24, 2008.
61. AOTR Supporting Plan Action Item 62, December 2007.
62. AOTR Supporting Plan Action Item 65, Assessment Study on the Feasibility and Desirability of Establishing a National-level Aviation Security Coordination Center, August 2007.
63. AOTR Supporting Plan Action Item 001, Operational Plans for Aviation Security Planning at National Special Security Events (NSSE) and Other Significant Security Events, September 2007.
64. Aviation Transportation System Recovery (ATSR) Supporting Plan, Implementation Plan for Aviation Transportation System Recovery, December 8, 2008.
65. Aviation Transportation Security System (ATSS) Supporting Plan Action Item 32, Shared Criteria for Flights of Interest, August 1, 2008.
66. Federal Aviation Administration, Department of Defense and Department of Homeland Security National Agreement (NAT)–120.
67. Federal Aviation Administration, Department of Defense and Department of Homeland Security National Agreement (NAT)–134.
68. Federal Aviation Administration Order 1200.22C, National Airspace System Data and Interface Equipment Used By Outside Interests, September 30, 2002.
69. Federal Aviation Administration. FAA Surveillance Strategy for NextGen, Briefing delivered by Jim Baird to Homeland Air Surveillance IPT, March 28, 2011
70. North American Aerospace Defense Agreement (United States-Canada), 2006.
71. North American Aerospace Defense Terms of Reference (United States-Canada), 2007.
72. FAA Order : JO 7110.65T Effective Date: February 11, 2010
73. National Institute of Standards and Technology (NIST) Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations, 2009.

Classified References

1. North American Air Surveillance Plan, Classified Annex, 26 Jul 2002 (Submitted by Air Surveillance Working Group (ASWG), but never fully staffed or approved.)
2. Homeland Air and Cruise Missile Defense of North America Joint Capabilities Document (JCD), 28 Nov 2005
3. Integrated Air and Missile Defense JCD, 21 Mar 2006
4. Integrated Air And Missile Defense Initial Capabilities Document (ICD), 1 Nov 2010
5. Integrated Air and Missile Defense CONOPS, 27 Feb 2009
6. N-NC Integrated Air and Missile Defense (IAMD) Roadmap, Ver.4 (still in development), (Projected Release Date) Aug 2011
7. Air Surveillance Gap Literature Review Final Brief, (PowerPoint), J8 Directorate, 31 March 2011
8. Tactical Employment Air Defense of the United States and Canada (ADUSCAN), 1 December 2010

Appendix B: Terms and Definitions

Note: *The definitions were derived from the reference documents located in Appendix A of the IS ConOps, complete with parenthetical numbers in bold—e.g.,* ***(1) (2) (3) (69) (70)****—that refer to the reference documents.*

Air Domain: The global airspace, including domestic, international and foreign airspace, as well as all manned and unmanned aircraft operating, and people and cargo present in that airspace, and all aviation-related infrastructures. **(1) (2) (35)**

Air Domain Awareness: The effective understanding of threats associated with the Air Domain that could impact the security, safety, or economy of the United States. **(1) (9) (10) (35)**

Air Domain Surveillance: The process for gathering information about the nature, position, or movement of a target or targets in the Air Domain (global airspace). Aviation security partners must regularly assess existing and future sensors requirements and, where appropriate, Federal departments and agencies must synchronize efforts to develop and integrate new and emerging technologies and capabilities to persistently monitor, detect, identify and track aircraft in those areas of national interest, both within and outside the United States. **(1) (7)**

Air Surveillance System: The sensors, automation systems and data distribution associated with the Air Domain. **(1) (2)**

Aircraft: A machine that can derive support in the atmosphere from the reactions of the air other than the reactions of the air against the earth's surface (as in the case of a rocket or missile). An aircraft can include a fixed-wing structure, rotorcraft, lighter-than-air vehicle, or a vehicle capable of leaving the atmosphere for space flight. **(8) (4)**

Airspace Situational Awareness: The shared cognizance and understanding of the present events—as well as an evaluation of the risks, threats, vulnerabilities and potential consequences—which transpire in the Air Domain. This activity is accomplished through an interconnected network of machines and personnel communicating data and information about the event in real time. **(2)**

Anomalous Activity Alert: An alert or warning notification in the form of a pop-up window, service report, email, or other computational signifier that indicates the non-normal behavior (anomalous activity) of an aircraft and which is automatically transmitted to ATO security and DHS, together with the ATM flight information indicating the aircraft's last know position.

Anomalous Behavior: Behavior that is non-normal, indicating that a person, object, or other entity should be put under surveillance. **(1) (2) (6) (8)**

Anomalous Operations: see **Non-Normal Operations**

Automatic Dependent Surveillance-Broadcast (ADS-B): An advanced surveillance technology that allows avionics to broadcast an aircraft's identification, position, altitude, velocity and other information. Since the aircraft's position is normally derived from the Global Positioning System (GPS) and transmitted at least once per second, the broadcasted position information is more accurate than most current radar-based position information. Additionally, the avionics provides uniquely specific flight parameter information with the broadcast of its surveillance position. The greater positional accuracy and ability to provide aircraft-derived flight parameters, in addition to position data, defines ADS-B as enhanced surveillance. These other parameters, such as directional vector, velocity, mid-term and long-term intent and other data are limited only by the equipment's capability, the communication data link capacity and the receiving system's capability. The accuracy and broadcast characteristics of ADS-B supports numerous cockpit-based and air traffic control applications. ADS-B-equipped aircraft with cockpit displays can receive ADS-B messages from other suitably equipped aircraft within the reception range resulting in an air-to-air and airport surface surveillance capability. ADS-B surveillance broadcasts can also be received by ground-based transceivers to provide air-to-ground and airport surface surveillance information for ATC and Traffic Flow Management (TFM) services and other functions such as fleet operations management, collaborative decision making and security functions. **(7)**

Automation System: A device that collects, analyzes, fuses and displays information from multiple sources and then displays and/or distributes the results. **(1)**

Aviation Transportation System: The system that includes the UNITED STATES airspace, all manned and unmanned aircraft operating in that airspace, all UNITED STATES aviation operators, airports, airfields, air navigation services and related infrastructure and all aviation-related industry. **(1) (2)**

Characteristic: An attribute or feature of an object, such as its position, speed, or course. **(1) (2)**

Consequence: The result of an attack on infrastructure assets reflecting level, duration and nature. Consequences can be measured in terms of loss of life, economic damage and/or psychological/political effects. **(2) (8)**

Controlled Airspace: An airspace of defined dimensions within which civilian air traffic control services are provided to control flights. **(13)**

Cooperative Air Vehicle: An air vehicle that acts in compliance with a United States agency, such as the FAA or United States Air Force. **(13)**

Cooperative Surveillance: Surveillance characterized by the requirement for equipping vehicles with functioning avionics that assist surveillance sensors to detect and identify the object. This type of surveillance is considered the routine and preferred method of airborne object detection because of the additional information it provides. **(1)**

Countermeasure: An activity implemented to mitigate risk. **(2)**

Cross Domain Security Gateways: Gateways comprised of trusted computing capabilities which serve as a guard between two different network security domains of classified and unclassified information, enabling the automated passing of data that meet systems security criterion between the domains for enhanced interagency information sharing and collaboration.

Data: Facts represented in a readable language (such as numbers, characters, images, or other methods of recording) on a durable medium. Data, on their own, carry no meaning. Empirical data are facts originating in or based on observations or experiences. A database is a store of data concerning a particular domain. Data in a database may be less structured or have weaker semantics (built-in meaning) than knowledge in a knowledge base. **(4)**

Detection Probability: The likelihood of position data reports (by type of object).

Dirigible: An airship that is a lighter-than-air vehicle—such as a blimp or Zeppelin—that can be steered by a rudder, propeller, or other form of thrust. **(13)**

Domestic Air Space: Airspace that overlies the continental land mass of the United States, plus Alaska, Hawaii and United States possessions. **(74)**

Enterprise Architecture (*Integrated Surveillance*): The organizing logic for business processes and Information Technology (IT) infrastructure associated with the capabilities, operational activities and identified relationships between and among the federal agencies, so as to bring about integrated surveillance. **(1) (5)**

Flight Data: The collection of attributes associated with each known and planned flight within the Air Domain. This may include dozens of data points such as aircraft type, aircraft identification and flight plan. **(1) (7)**

Flight Object: A set of flight-specific, data elements available throughout the duration of the flight, both to the user and the affected service providers across the NAS. The flight object is contained in the message set, which may contain Flight Profile and Flight Trajectory information. These message set data elements may consist of flight information such as flight route, discrete identification code, preferred trajectory, aircraft weight, type position, runway preference, gate assignment, etc. Flight Profile information includes a complete set of user preferences for climb, descent, cruise and other operational preferences. Flight Trajectory information includes the four-dimensional path of the flight expressed at the level of performance the flight is capable of achieving. **(7)**

Flight Track: A representation of an aircraft's position as it moves from its initial location and altitude (typically the departure airport) to its final location and altitude (typically its destination airport). **(1) (2) (6) (8)**

Hostile Intent: The threat of imminent use of force by a foreign force, terrorist(s), or organization against the United States and U.S. national interests, U.S. forces and, in certain circumstances, U.S. nationals, their property, U.S. commercial assets and other designated non-U.S. forces, foreign nationals and their property. When hostile intent is present, the U.S. may use proportional force, including armed force, in self-defense by all necessary means available to deter or neutralize the potential attacker or, if necessary, to destroy the threat. A determination that hostile intent exists and requires the use of proportional force in self-defense must be based on evidence that an attack is imminent. Evidence necessary to determine hostile intent will vary depending on the state of international and regional political tension, military preparations, intelligence and indications and warning information. **(13)**

Instrument Flight Rules: Regulations and procedures for flying aircraft by referring only to the aircraft instrument panel for navigation. **(29)**

Integrated Aviation (Air) Surveillance: The integration of information from cooperative and non-cooperative surveillance systems to create a user-defined operational picture (from common information) of real or near-real time situation for safety, security and efficiency. **(1) (7)**

Integrity: Independent determination of data veracity. In this context, a quality whereby data and/or information is considered consistent, whole and accurate, usually as such data and/or information is involved in multiple processes and uses. **(1) (2)**

Intelligence: The product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available data and information concerning foreign countries or areas. **(1) (2)**

Intelligence Community: The community comprised of the Office of the Director of National Intelligence; the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; other offices within the Department of Defense involved in the collection of specialized national intelligence through reconnaissance; the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation and the Department of Energy; the Bureau of Intelligence and Research of the Department of State; the Office of Intelligence and Analysis of the Department of Treasury; the Office of Intelligence of the Coast Guard in the Department of Homeland Security; the intelligence elements of the Drug Enforcement Administration; and such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the Intelligence Community. **(1)**

Intent (*Flight*): The information associated with a flight, including the aircraft's filed flight plans, on-board Flight Management System (FMS) trajectories representing intent and current/predicted positions, preferred routes and altitudes, broadcast information, preferred runway, gate assignment, pushback and taxi information **(6)**

Intent (*Purpose*): An aim or design to execute a specified course of action. **(13)**

Interdiction: (1) A military action to divert, disrupt, delay, or destroy the enemy's military capability before it can be used effectively against friendly forces, or to otherwise achieve objectives. (2) A law enforcement activity conducted to divert, disrupt, delay, intercept, board, detain, seize or arrest, as appropriate, vessels, vehicles, aircraft, people and cargo. **(13)**

Mode of Operation, Augmented: A mode of operation whereby the normal mode of operation is enhanced with additional capability, when special circumstances require. This augmented mode would also serve to mitigate degradation due to loss of facilities.

Mode of Operation, Degraded: A mode of operation whereby a reduced level of capability results when some or all of the sensors, digital components, communication links, etc., are degraded due to either natural or manmade causes.

Mode of Operation, Exercise: A mode of operation whereby the system is exercising scenarios. This mode is done for the training of operators, supervisors and managers in a realistic "train as you fight" environment.

Mode of Operation, Nominal: see **Normal Operations**

Mode of Operation, Off-Nominal: see **Non-Normal Operations**

Mode of Operation, Training: A mode of operation utilized for educating and training operators.

Multilateration: The process involved in locating and tracking a target through computation of the difference of time in the arrival of a signal emitted from the target to multiple receivers. **(7)**

National Airspace System: The common network of U.S. airspace including air navigation facilities, equipment, services, airports or landing areas, aeronautical charts, information/services, rules, regulations, procedures, technical information, manpower and material. Also, please see **Domestic Air Space**. **(6), (7), (8), (29), (53)**

National Airspace System Automation: An automated anomaly analysis algorithm that will precipitate anomaly alerts. In order to better identify potential threats and thereby prevent catastrophic events, the automation will detect and correlate anomalous travel patterns into a profile. **(1)**

Net-Centric Information Management Service: see **Service**

Net-Centric Operations: An approach which allows for the integration of all existing and future surveillance inputs through a collection of self-synchronized networks. **(10)**

Net-Centricity: A robust, globally interconnected network environment in which data and information are shared in a timely and consistent manner among users, applications and platforms. **(8)**

Network Enabled Architecture: Computational architecture utilizing net-centric operations. **(10)**

Next Generation Air Transportation System: A comprehensive transformation and evolution of our nation's air transportation infrastructure, as well as how the infrastructure is developed, operated, and maintained, primarily through new and updated:

- **Automation:** Integrated information systems are needed that provide advanced trajectory, separation, capacity, flow contingency and security management functions
- **Infrastructure:** Advanced technologies are needed that provide integrated communication, navigation, surveillance and security infrastructure services
- **Processes:** New automation and infrastructure requires new and revised responsibilities and integrated processes to provide increased capacities and efficiencies
- **Collaboration:** Industry and government need to work together in new ways to define, fund, develop, implement, govern, and operate NextGen technologies, processes, and policies
- **Integrated Operations:** NextGen operational processes and technologies require the integration of safety, security and environmental requirements as core components
- **Information Sharing:** Integrated operations require the broad sharing of information across many organizations and systems in an open, yet secure, manner
- **Knowledge Development:** NextGen can benefit from formal and informal networks to enhance creation of new knowledge, resulting in more innovative problem solving.

The future of our nation's ability to move people and goods in a safe, secure, efficient and environmentally responsible manner depends upon successful implementation of NextGen. NextGen will collect, integrate, fuse, analyze and disseminate cooperative and non-cooperative aviation surveillance information and other aviation security-associated information. **(6)**

Non-Cooperative Active Surveillance: A type of surveillance that uses a transmitter to send a radio-frequency (RF) field that reflects off the airborne object and is detected by a receiver collocated with the transmitter or located elsewhere. The distance to the object is determined by the time it takes for the RF to make the round trip and the angle is determined by the position of the antenna. This type of surveillance works even if the airborne object has no cooperative systems on board. **(1) (6)**

Non-Cooperative Air Vehicle: An air vehicle that does not act in compliance with a U.S. agency, such as the FAA or Department of Defense. **(1) (6)**

Non-Cooperative Surveillance: Surveillance that does not require that vehicles be equipped with functioning avionics that assist surveillance sensors to detect and identify the object. Non-cooperative surveillance is required for defense, security and law enforcement missions. It is also required for ATC in high-density terminal areas and must complement other ATC needs when the required cooperative surveillance capability is lost. **(1)**

Non-Normal Operations (*Anomalous Operations, Off-Nominal Operations*): When services, systems and functions—such as the Broadcast Services System (BSS)—are not available and/or operational, and all services cannot be provided, depending upon the implementation segment. **(7)**

Normal Operations (*Nominal Operations*): When services, systems and functions—such as BSS—are available and/or operational and all services can be provided, depending upon the implementation segment. In the case of BSS, for example, this status also assumes that the interfacing systems providing the surveillance reports for Traffic Information Service-Broadcast (TIS-B) and weather and aeronautical data for Flight Information Service-Broadcast (FIS-B) are operational and providing that data. Otherwise, the TIS-B and FIS-B services would not be available. **(7)**

Off-Nominal Operations: see **Non-Normal Operations**

Purpose: see **Intent**

Required Surveillance Performance: a means of specifying surveillance quality necessary to support operational requirements. RSP is quantified by metrics that can vary by mission needs and airspace volumes. A national integrated surveillance service capability will nominally provide capability to satisfy the most demanding RSP for an airspace volume. The RSP concept describes a means of specifying surveillance quality necessary to support operational requirements.

The surveillance service should monitor performance and include a means of reporting achieved surveillance performance to operators. The integrated surveillance service may achieve surveillance performance that might fall short of designed RSP due to system faults, atmospheric conditions, maintenance activities or other factors. Operator notification of achieved surveillance performance enables execution of contingency plans (such as fallback to reduced capability operations) and enables initiation of activities to repair or temporarily replace failed systems.

The surveillance service should be planned to operate in degraded modes, which support operations that remain possible under a lower RSP. This situation enables design of a service where the cost of high service availability may be reduced in selected service volumes, while also enabling development of a system that will provide continuity of operations, retaining a usable surveillance capability in the event of equipment failure or other causes that disrupt availability.

The following attributes of surveillance data elements and reports define RSP:

- Availability—likelihood of surveillance service for a specified volume;
- Update Period—time between position estimates;
- Detection Probability—likelihood of position data reports (by type of air vehicle);
- Continuity—probability of a series of correlated reports;
- Integrity—independent determination of data veracity;
- Accuracy—precision of position or velocity; and
- Latency—data age when available for display or other use.

(1) (2) (6) (8)

Risk: A measure of potential harm that encompasses threat, vulnerability and consequence. **(2) (8)**

Risk Level: A metric used to describe briefly the potential severity of the subject risk posed to the United States and its interests. **(2)**

Risk Profile: A summary of threat, consequence and vulnerability characteristics dynamically associated with a flight object. This information is compiled with the aid of automation and analyzed by DHS, ATO and other security partners. **(2)**

Security Volumetric Expression: The volume of protected area around an asset or an event in response to a security risk profile. **(2)**

Separation: A minimum distance to keep an aircraft safe from other aircraft, terrain, obstacle, the ground, or specified airspace. **(2)**

Service (*Net-Centric Information Management*): A computational mechanism that: (a) enables access to one or more capabilities using a prescribed interface; (b) is composed of operations (e.g., create, read, update, delete) usually having a common, functional goal; (c) is offered by one system/software application to another system/software application; (d) is carried out via the electronic exchange of data and information over an enterprise network; and (e) follows a precise set of rules and protocols according to a service definition (a machine and human-readable, technical description of the service). **(6)**

Situational Awareness: The shared cognizance and understanding of the present events—as well as an evaluation of the risks, threats, vulnerabilities and potential consequences—which transpire in some domain. This status is accomplished through an interconnected network of machines and personnel communicating data and information about the event in real time. **(2) (8)**

Stakeholder: A person or organization that has a legitimate interest, or vested interest in a project or entity; anyone with an interest (or stake) in what the entity does. The security and aviation organizations involved in or affected by security activities. **(2) (4) (8)**

Surveillance: The process for gathering information about a nature, position, or movement of a target (e.g., tracking the position and vector of an aircraft or a vessel). **(1) (2)**

Surveillance Community: The surveillance mission partners, industry and academia. **(1) (2)**

Suspicious Activity Report: A report generated by a person or machine that results from suspicious behavior and includes key information about the flight, the aircraft operator, the air traffic management position detecting the suspicious activity, and the aircraft's location. **(2)**

Suspicious Behavior: Behavior where (a) the intention is unclear (intentionally or inadvertently), or (b) there is reason to doubt the intention or execution of some behavior, indicating that a person, object, or other entity should be put under surveillance. **(1) (2) (6) (8)**

Target: An object of surveillance. **(1) (2) (7)**

Threat: The likelihood of an attack on a particular asset based on intent and capability of the adversary. **(2)**

Track: The projection on the earth's surface of the path of an aircraft, the direction of such path at any point is usually expressed in degrees from North (True, Magnetic, or Grid). **(7)**

Trajectory: A four-dimensional representation of an aircraft's predicted future position as it moves from its initial location and altitude (typically the departure airport) to its final location and altitude (typically its destination airport). It is also described as the time ordered sequence of points that describe an aircraft's route of flight in the horizontal, vertical and time dimensions. **(2) (6)**

Update Period: The time between position estimates of an aircraft. **(1)**

User: Any person or agency (here, specifically, DoD, DOT, DOC, DHS, ODNI) that utilizes the work-sites, terminals and systems associated with NAS and NextGen surveillance, such as an operator, agent, or air traffic controller.

User-Defined Operational Picture: The implementation of information standards ensuring that common representations of information are applied in a way that people can understand and use the information. **(2)**

Visual Flight Rules: Rules that govern the procedures for conducting flight under visual conditions. **(29)**

Vulnerability: The weakness in the design, implementation, or operation of an asset or system, which can be exploited by an adversary or disrupted by a natural disaster. **(2)**

Weather Surveillance: The means, through human and automated sensors, to measure *in situ* characteristics of the atmosphere. It can be done remotely by space-, air- and land-based systems, including on-board sensors, radar and satellite technologies. **(1) (6)**

Appendix C: Acronyms

4D: Four-Dimensional

ADA: Air Domain Awareness

ADAB: Air Domain Awareness Board

ADAPT: Automatic Detection and Processing Terminal

ADS: Automatic Dependent Surveillance

ADS-A: Automatic Dependent Surveillance-Addressed

ADS-B: Automatic Dependent Surveillance-Broadcast

ADSII: Air Domain Surveillance and Intelligence Integration

ADSUSCAN: Air Defense of the United States and Canada

AEW: Airborne Early Warning

AIS: Automatic Identification System

AMOC: Air and Marine Operations Center

AMOSS: Air and Marine Operations Surveillance System

ANSP: Air Navigation Service Provider

AOR: Area of Responsibility

AOTR: Aviation Operational Threat Response

ASR: Airport Surveillance Radar

ASWG: Air Surveillance Working Group

ATC: Air Traffic Control

ATM: Air Traffic Management

ATO: Air Traffic Organization

ATS: Aviation Transportation System

ATSA: Aviation and Transportation Security Act

ATSR: Aviation Transportation System Recovery

ATSS: Aviation Transportation Security System

AWACS: Airborne Warning and Control System

BCS-F: Battle Control System - Fixed

BSS: Broadcast Services System

C2: Command and Control

CIKR: Critical Infrastructure and Key Resource

CIO: Chief Information Officer

CIP: Critical Infrastructure Protection

CONPLAN: Concept Plan

ConOps: Concept of Operations

CONUS: Continental United States

COOP: Continuity of Operations

DEN: Domestic Events Network

DGAC: Director General of Civil Aeronautics

DHS: Department of Homeland Security

DOC: Department of Commerce

DoD: Department of Defense

DOJ: Department of Justice

DOT: Department of Transportation

DSCA: Defense Support of Civil Authorities

EA: Enterprise Architecture
EADS: Eastern Air Defense Sector
ESCAT: Emergency Security Control of Air Traffic
ETMS: Enhanced Traffic Management System
EUROCONTROL: European Organisation for the Safety of Air Navigation
FAA: Federal Aviation Administration
FAM(S): Federal Air Marshal (Service)
FFDO: Federal Flight Deck Officer
FFT: Friendly Force Tracker
FIS-B: Flight Information Service-Broadcast
FMS: Flight Management System
FY: Fiscal Year
GA: General Aviation
GEOINT: Geospatial Intelligence
GPS: Global Positioning System
HUMINT: Human Intelligence
IAMD: Integrated Air and Missile Defense
IC: Intelligence Community
ICD: Initial Capabilities Document
ICE: Immigration and Customs Enforcement
IFR: Instrument Flight Rules
IP: Internet Protocol
IPT: Integrated Process Team
IS ConOps: Integrated Air Surveillance Concept of Operations
ISE: Information Sharing Environment
ISEA: Integrated Surveillance Enterprise Architecture
ISE-SAR: Information Sharing Environment-Suspicious Activity Report
ISR: Intelligence, Surveillance and Reconnaissance
ISST: Integrated Surveillance Study Team
IT: Information Technology
JCD: Joint Capabilities Document
JIAMDO: Joint Integrated Air and Missile Defense Organization
JPDO: Joint Planning and Development Office
LRR: Long Range Radar
MANPADS: Man-Portable Air Defense System
MASINT: Measurement and Signature Intelligence
MSAW: Minimum Safe Altitude Warning
MSL: Mean Sea Level
NAASP: North American Air Surveillance Plan
NAS: National Airspace System
NASA: National Aeronautics and Space Administration
NAT: National Agreement
NATO: North Atlantic Treaty Organization
NCR: National Capital Region
NCRCC: National Capital Region Coordination Center
NEO: Network Enabled Operation

NEWP: NextGen Executive Weather Panel
NEXRAD: Next Generation Weather Radar
NextGen: Next Generation Air Transportation System
NIST: National Institute of Standards and Technology
NOAA: National Oceanic and Atmospheric Administration
NORAD: North American Aerospace Defense Command
NSAS: National Strategy for Aviation Security
NSPD-47/HSPD-16: National Security Presidential Directive-47/Homeland Security Presidential Directive-16
NSSE: National Special Security Event
OAG: Official Airline Guide
ODNI: Office of the Director of National Intelligence
OFCM: Office of the Federal Coordinator for Meteorology
OMB: Office of Management and Budget
OpsCon: Operational Concept
OSINT: Open Source Intelligence
OSTP: Office of Science & Technology Policy
Pt–to-Pt: Point to Point
RF: Radio Frequency
RSP: Required Surveillance Performance

RTAP: Remote Tactical Air Picture
SAR: Suspicious Activity Report
SIF: Special Interest Flight
SIGINT: Signals Intelligence
SOA: Service-Oriented Architecture
SPC: Senior Policy Committee
SRR: Short Range Radar
SSA: Shared Situational Awareness
STARS: Standard Terminal Automation Replacement System
TARS: Tethered Aerostat Radar Systems
TFM: Traffic Flow Management
TFR: Temporary Flight Restriction
TIS-B: Traffic Information Service-Broadcast
TOI: Track of Interest
TSA: Transportation Security Administration
TSOC: Transportation Security Operations Center
UAS: Unmanned Aircraft Systems
UDOP: User Defined Operational Picture
U.S.: United States
USAF: United States Air Force
USCG: United States Coast Guard
USNORTHCOM: United States Northern Command
USSS: United States Secret Service
VFR: Visual Flight Rules
WSR: Weather Surveillance Radar

Appendix D: Surveillance Capability Parameters ***(Published Separately)***